

HCFA YEAR 2000
BUSINESS CONTINUITY PLAN (BCP)
HANDBOOK
Steps 1 to 6, Part 1

TABLE OF CONTENTS

Table of Contents.....	i
1.0 Introduction.....	1-1
1.1 THE YEAR 2000 (Y2K) PROBLEM.....	1-1
1.2 THE ROLE OF CONTINGENCY PLANNING.....	1-2
1.3 THE PRIMARY OBJECTIVE: BUSINESS CONTINUITY.....	1-2
1.4 THE BUSINESS CONTINUITY PLANNING PROJECT.....	1-4
1.5 THE WORKGROUP BUSINESS CONTINUITY PLANNING REQUIREMENTS.....	1-5
1.6 OVERVIEW OF THE BUSINESS CONTINUITY PLANNING PROCESS.....	1-6
2.0 Step 1: Isolate and Document Critical Business Processes/Functions.....	2-1
2.1 LINKING DAY-TO-DAY OPERATIONS TO THE MISSION.....	2-1
2.2 IDENTIFYING AND DEFINING BUSINESS FUNCTIONS AND ASSESSING THEIR CRITICALITY.....	2-2
2.2.1 ISOLATING CRITICAL BUSINESS FUNCTIONS.....	2-3
2.2.2 CRITERIA FOR ASSESSING BUSINESS FUNCTION CRITICALITY.....	2-4
2.2.3 CRITICALITY ASSESSMENT.....	2-6
3.0 Step 2: Analyze and Document Resources and External Factors.....	3-1
3.1 CATEGORIES OF DEPENDENCIES.....	3-1
3.2 BUSINESS PROCESS RESOURCE DEPENDENCIES.....	3-2
3.2.1 IDENTIFYING DEPENDENCIES.....	3-2
3.2.2 ASSESSING THE LEVEL OF DEPENDENCIES.....	3-3
4.0 Step 3: Establish and Document Risk Conditions.....	4-1
4.1 AGENCY-WIDE RISK SCENARIOS AND POLICY.....	4-1
4.2 ESTABLISH RELATIONSHIP BETWEEN AGENCY-WIDE SCENARIOS AND WORKGROUP RISK CONDITIONS.....	4-2
4.3 RISK IDENTIFICATION AND ASSESSMENT.....	4-3
5.0 Step 4: Perform and Document Business Impact Analysis.....	5-1
5.1 FOCUS OF THE BUSINESS IMPACT ANALYSIS.....	5-1
5.2 RISK IDENTIFICATION AND ASSESSMENT.....	5-1
6.0 Step 5: Develop, Evaluate, and Document Contingency Strategies.....	6-1
6.1 IDENTIFYING LOGICAL PROCESS GROUPINGS FOR CONTINGENCY PLANNING.....	6-1
6.2 DEVELOPING POTENTIAL ALTERNATE STRATEGIES.....	6-1
6.3 EVALUATING, DOCUMENTING, AND SELECTING ALTERNATE STRATEGIES.....	6-4
7.0 Step 6, Part 1: Draft Contingency Plans.....	7-1
7.1 DEVELOPING A PROJECT PLAN.....	7-1
7.2 DEVELOPING PLAN PROCESSES AND PROCEDURES.....	7-2
7.3 DRAFTING THE CONTINGENCY PLAN.....	7-3
7.4 DEVELOPING AND DOCUMENTING CONTINGENCY PLAN ADMINISTRATIVE PROCEDURES.....	7-3
8.0 Steps 5 & 6: Plan Risk Mitigation and Mitigate Risks.....	8-1
8.1 ESTABLISHING RISK MITIGATION TIMELINE.....	8-1
8.2 DEVELOPING POTENTIAL ALTERNATE STRATEGIES.....	8-2
8.3 EVALUATING, DOCUMENTING, AND SELECTING ALTERNATE STRATEGIES.....	8-3
8.4 IMPLEMENTING THE RISK MITIGATION PLAN.....	8-3

9.0 Step 6, Part 2: Test and Finalize Contingency Plans*To Be Distributed At A Later Date*

- 9.1 TESTING, MODIFYING, AND FINALIZING THE CONTINGENCY PLAN
- 9.2 TRAINING PERSONNEL
- 9.3 MAINTAINING THE CONTINGENCY PLAN

10.0 Step 7: Establish Readiness for Contingency Plan.....*To Be Distributed At A Later Date*

Appendix A: Glossary.....	A-1
Appendix B: Business Continuity and Contingency Planning Template.....	B-1
Appendix C: Costing Worksheets for Y2K Risk Mitigation and Contingency Plans.....	C-1
Appendix D: Final Contingency Plan Outline.....	D-1
Appendix E: Final Risk Mitigation Plan Outline.....	E-1

The Basic Why & How of Business Continuity Planning

1.0 INTRODUCTION

1.1 The Year 2000 (Y2k) Problem

Computer programs designed and developed over the past several decades have typically used only two digits to record the year (e.g., using “98” to represent 1998). This was originally done to reduce the size of database requirements making data storage more efficient and less expensive. Programmers believed that this approach would not create processing problems until the turn of the century, and because they also anticipated that the systems they designed would be replaced well before that time, the potential danger in adopting this method was not viewed as significant. Unfortunately however, such predictions of widespread replacement of systems affected by the two digit dating convention have not proven accurate. The use of such systems has become even more widespread and many of the systems built 20 – 25 years ago are still in use today.

Section Overview

- 1.1 The Year 2000 (Y2K) Problem
- 1.2 The Role of Contingency Planning
- 1.3 The Primary Objective: Business Continuity
- 1.4 The Business Continuity Planning Project
- 1.5 Contingency Plan Workgroup Business Continuity Planning Requirements
- 1.6 Overview of the Business Continuity Planning Process

The Year 2000 (Y2k) problem occurs when attempts are made to process data for the year 2000 or after using the last two digits, because most computer systems in use today interpret a “00” entry as representing the year 1900 rather than the year 2000. The result is that when this condition is experienced, affected systems will either compute erroneous information or simply stop working. For example, suppose a computer system is used to perform age calculations in order to determine Medicare eligibility for an individual born on January 1, 1935. If the system is not affected by the Y2k problem, a calculation will be performed in 2000 in which the individual's date of birth is subtracted from the current date. When 1935 is subtracted from 2000 the result is 65 and the individual will be determined to be eligible for Medicare benefits. However, if the system is affected by the Y2k problem, 35 will be subtracted from 00. The result is that the computer will erroneously believe that the individual is -35 years old and therefore not eligible for Medicare benefits. The Y2k problem is further complicated by the fact that 2000 is a leap year and by additional programming conventions such as the use of 9/9/99 to signify computer program termination.

While the Y2k problem is simple in concept, the immense size and scope of the effort (affecting both system and infrastructure elements within almost every level of government and component of the private sector) has raised doubts whether all necessary corrections can be accomplished in time.

1.2 The Role of Contingency Planning

“Contingency planning is one of the most critical, yet most overlooked, areas of a Year 2000 initiative.”

**William M. Ulrich,
Tactical Strategy
Group, Inc.**

Although most Federal Department/Agency Y2k program management plans have identified the need to develop contingency plans, many government-wide efforts in this area are still in the initial stages of development. To date, the focus of the Y2k programs has been on bringing systems and infrastructure elements into compliance (i.e., the ability to accurately process and exchange date/time data and/or to continue performing correctly from, into, and between the 20th and 21st centuries), rather than on ensuring that critical business functions are able to continue without interruption. However, recent General Accounting Office (GAO) and Office of Management and Budget (OMB) guidance have expanded Y2k program requirements to include contingency planning. Basically, contingency planning should, as a minimum, provide for the continued performance of an agency's critical business functions by providing planned operational alternatives which can be implemented when:

- ☐ Information technology (IT) and/or non-IT systems, that are believed to be Y2k compliant, fail in actual operations;
- ☐ IT and non-IT systems are not compliant by their established “need date;”
- ☐ Supporting IT and physical infrastructure elements are unavailable (e.g., networks, data and voice communications, electric power, transportation, fire safety systems, etc);
- ☐ IT or non-IT failures in upstream systems cause change (non-compliant format or significantly different volume) of inputs; and,
- ☐ Threats from external events compound one or more of the above situations.

1.3 The Primary Objective: Business Continuity

Early approaches to contingency planning primarily emphasized recovery of resources, such as ADP services, facilities, etc., following a contingency, such as a fire or natural disaster. Over time, planners realized that the recovery of such resources, while important, was the wrong focus, because waiting for these resources to be restored before mission critical functions could be performed often had a long-term detrimental effect on operations. An extensive number of commercial operations could not survive an extended outage, and many public agencies would expend large amounts of staff hours and funding to recover functional capabilities and clear processing backlogs. It was recognized that normally there is work-around that can be implemented to allow the continued performance of critical business functions. Although there

would be a reduced level of productivity, public institutions could continue to perform mission requirements, and commercial enterprises could sustain the production of essential sales revenue.

Essentially, a business function relies on input and resources to perform its processes, which produces products or services under normal events. See Figure 1.1.

Contingencies may be caused by the inputs, external events or resources used in the performance of a business function (e.g., information systems are unusable, ADP and other equipment is damaged or corrupted, facilities are lost, etc). With the changes (errors in content or extra volume) of inputs, threats from external events, or loss of its supporting resources, the business function may stop producing products or providing service. See Figure 1.2.

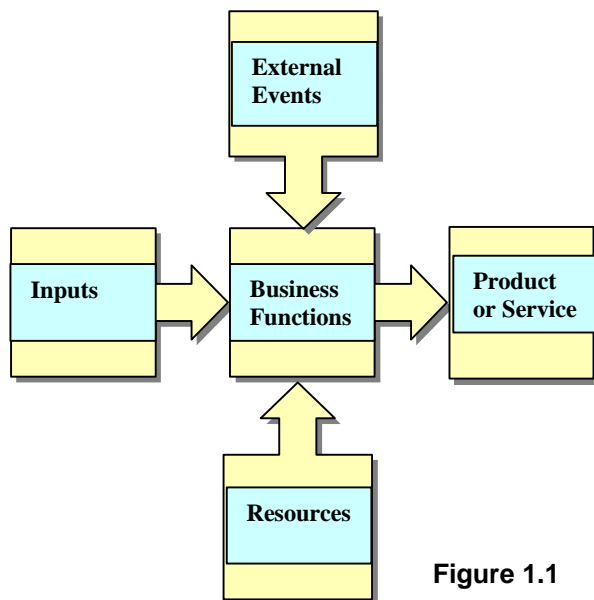


Figure 1.1

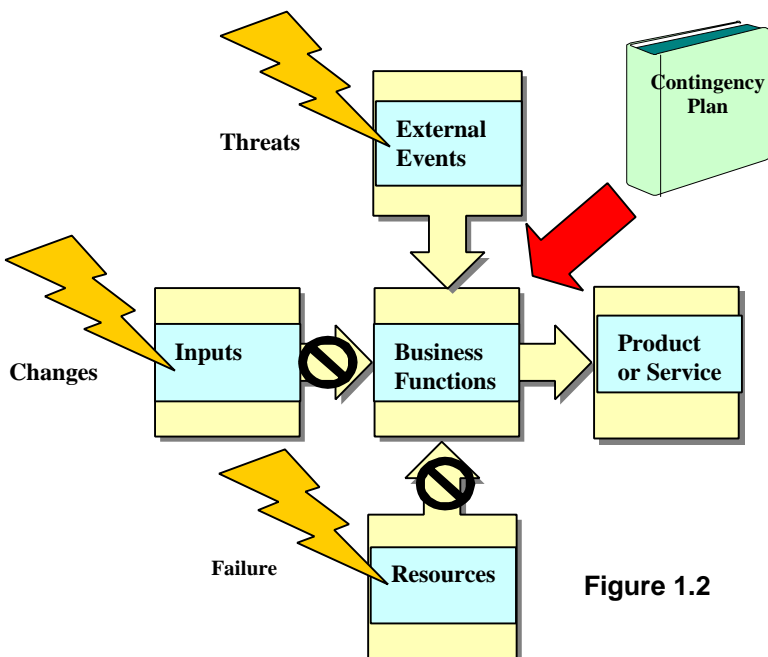


Figure 1.2

Contingency plans provide pre-planned strategies to compensate and work around the change of inputs, threats from external events and loss of resources. They allow the organization to accomplish its critical business functions and to continue to supply its essential product or service. Contingency procedures remain in effect until normal operations are restored.

HCFA's Business Continuity Planning efforts include both risk mitigation and contingency planning elements. The risk mitigation efforts are aimed at reducing the likelihood that risk conditions will actually occur. While current information applications and infrastructure are

being renovated to be Y2K compliant, contingency plans will be developed with the assumption that all renovation may not be completely implemented. See Figure 1.3.



Figure 1.3

1.4 The Business Continuity Planning Project

The HCFA Year 2000 Executive Committee has established a Business Continuity Planning Project and established the Division of Agency Contingency Planning (DACP) to be responsible for the development of Agency-wide contingency plans. The goal is to ensure that HCFA can deliver an acceptable level of health care financing for its beneficiaries in the event of Y2k failure. The guiding principles set for the planning work are to:

1. Continue payment;
2. Safeguard the Trust Funds;
3. Protect quality of care for the Medicare beneficiaries; and,
4. Sustain beneficiary entitlement and enrollment.

With the goal and guiding principles determined, HCFA formed several workgroups to address cross-component business functions. These workgroups are:

1. Program integrity;
2. Payment operations;
3. Quality of care;
4. Enrollment;
5. Managed care;
6. Litigation; and,

7. Telecommunications.

Each workgroup cuts across components and has representatives from multiple components. The Telecommunications and Litigation workgroups are not directly related to a specific business process. The first five workgroups were formed to address business continuity for a specific business process. We have prepared this handbook to guide the contingency planners through the business continuity planning process and preparation of a business continuity plan comprised of risk mitigation plans and contingency plans. This handbook supports and supplements the project's workshop training sessions. A copy of the project plan is available on the HCFA Year 2000 Web site, or through the DACP Staff.

The DACP consists of four teams, namely:

1. Contingency Planning Support Team: This team provides direct support to all workgroups. It facilitates the business continuity planning process and conducts training. It also reviews the information gathered by the workgroups.
2. Risk Management and Data Analysis Team: This team stores and analyzes the information gathered by the workgroups into a database.
3. Scenario Development and Policy Analysis Team: This team develops Agency-wide risk scenarios and develops policies and strategy to address the risk scenarios on the macro level. The scenarios developed by this team will be compared with the risk conditions (see Step 3) developed by each workgroup. The policies and strategy will be used to guide the development of contingency plans for specific risks.
4. Project Management and Documentation Team: This team tracks the project schedule and development of contingency plans.

Science Applications International Corporation (SAIC) provides contract support to develop the contingency planning process and training materials, establish the database, track the schedule, and provide technical consultation to HCFA.

1.5 Contingency Plan Workgroup Business Continuity Planning Requirements

Each Contingency Plan Workgroup (Workgroup) will prepare contingency plans which cover its critical business functions and provide operational responses to the potential Y2k change of input, threats from external events, and loss of supporting systems and infrastructure. HCFA's Business Continuity Plan will be comprised of the aggregated contingency plans. This handbook, and the associated workshop training seminars, will provide planners with the guidance needed to accomplish these requirements. The key milestones for the preparation of BCPs are as follows:

- ☐ Completion of draft contingency plans (completely coordinated within the Workgroups and ready for testing) by March 31, 1999.
- ☐ Testing, modification, validation, and finalization of contingency plans and training of all responsible owners and contingency plan personnel, by June 30, 1999.

1.6 Overview of the Business Continuity Planning Process

The major steps involved in business continuity planning are outlined in Figure 1.4. It is not always necessary to fully complete the activities required in one step before moving on to the next. Therefore, it will be possible to have different people working on activities associated with several different steps in the process at the same time. Proactive management is required to ensure that an organized approach is maintained, and that there is economy and efficiency applied in the actions being performed.

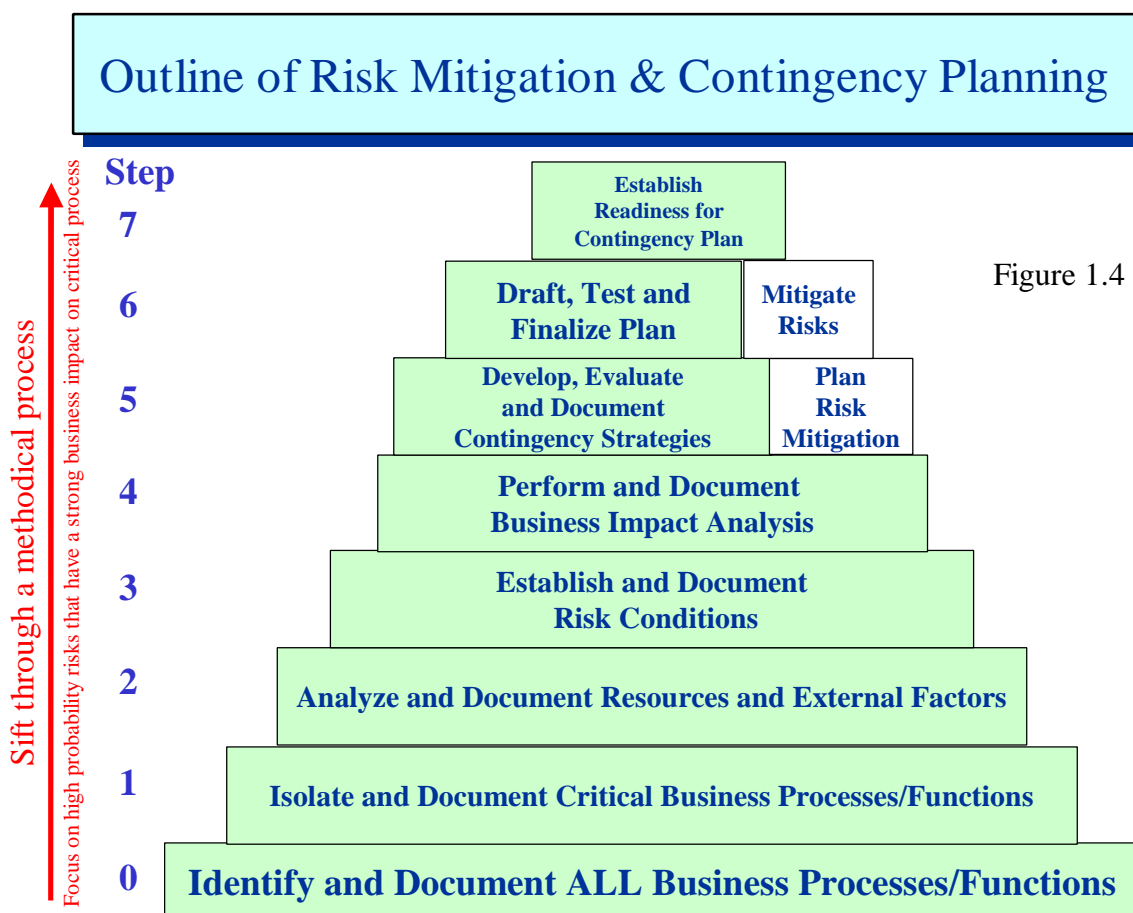




Figure 1.4

In essence, the contingency planning process sifts through the steps to focus only on risks that will have high probability of occurrence and high business impact on critical business processes. The activities associated with contingency planning will be discussed in greater detail in the sections that follow and in the training workshops scheduled as part of the contingency planning effort. All information gathered in each step will be captured in a Microsoft Access Database. The Business Continuity and Contingency Planning Template (Template), Appendix B, will be used as a vehicle for all workgroups to submit the necessary information. After the Contingency Planning Support Team reviews the information, it will be entered into the database. Then, reports can be generated from the database to facilitate effective planning.

	<i>Input</i>	<i>Business Continuity Planning</i>	<i>Output</i>	
	A description of each business function performed by the Agency that identifies inputs, processes and outputs; core business areas supported; interdependencies with other offices, external agencies, and functions.	1. <i>Isolate and Document Critical Business Processes/Functions</i> – Information collected for each business function is compared to established criteria to determine its criticality.	Identification of those business functions performed by the Agency that are critical to the accomplishment of identified core business areas -- and therefore essential to the effective performance of the overall Agency's mission.	
	Identification of the inputs, external events, and resources (human, system and infrastructure) that are used in the performance of each of the Agency's critical business functions identified in Step #1.	2. <i>Analyze and Document Input, External Events, and Resources</i> – Inputs and Resources used by each critical business function are documented and analyzed to determine function's degree of dependency on each. External events are analyzed to identify potential threats.	An analyses of critical business function input and resource dependency which can be used to assess the impact if inputs are changed or if resources are lost due to Y2K or other contingency. Also, an analysis of threats from external events.	
	Inputs include: the input and resource analysis from Step #2; and, Agency-wide risk scenarios outlining potential macro-level contingencies affecting IT systems, IT infrastructure; telecommunications; and the physical infrastructure.	3. <i>Establish and Document Risk Conditions</i> – Analysis of input, external events and resource dependency is compared to Agency-wide scenarios to develop risk conditions identifying potential impacts on critical business functions.	Identification, for each critical business function, of the specific inputs, external events, and resources that will be affected by the contingency conditions defined in the Agency-wide risk scenarios. Risk conditions are developed for each risk scenarios. Similarly, use the risk conditions identified in the workgroups to validate and add risk scenarios.	
	Risk conditions developed for each critical business function.	4. <i>Perform and Document Business Impact Analysis (BIA)</i> – Risk conditions are analyzed and the specific impact of their loss is assessed.	An analysis of the specific impact of each risk condition on the ability to perform critical business functions. Impacts are defined as to their effect on the function's inputs, processes and outputs and its overall ability to support core business areas.	
	The BIA developed for each critical business function.	5. <i>Develop and Document Alternate Continuity Strategies</i> – The specific impacts identified in the BIA are analyzed to identify alternate approaches for working around problems and continuing the performance of critical business functions, despite the change of inputs, threats from external events, and loss of resources.	An alternate continuity strategy is developed for each of the risk conditions applicable to the Agency's critical business functions.	

Inputs include: the business function analysis (Step #1), resources analysis (Step #2), contingency scenarios (Step #3), BIA (Step #4); and alternate continuity strategies (Step #5).	6. <i>Draft, Test and Finalize the Written Business Continuity Plan</i> – Outputs from Steps #1-4 are used to document the background for the BCP and to define the potential contingency conditions and impacts which the Agency may experience. The alternate continuity strategies are broken down into the processes and procedures required to execute the BCP.	A written and finalized Workgroup Business Continuity Plan.
Final BCP	7. <i>Establish and Track Implementation Requirements</i> – The BCP is analyzed to determine, document and procure any special requirements that will be necessary to properly execute its processes and procedures.	Output of the final step in the process will be a list of the supplies, equipment, support, etc. that will be needed to execute the BCP, and a log to maintain status of their procurement.

Step 1: Isolate and Document Critical Business Processes/Functions

2.0 SECTION INTRODUCTION

The first step in the contingency planning process is to isolate those Agency business functions which are considered critical. The criticality of any function/process of an organization is ultimately determined by the extent of its contributions to the attainment of the organization's overall mission or business goals. In general, not all of the business functions performed by an office should be rated as critical. To properly identify critical business functions, the characteristics of each business function performed by the Agency must be defined and compared to criteria that helps to assess and gauge its contribution to the Agency's overall mission performance. This link between day-to-day operations and the organization's overall mission is discussed in greater detail in Subsection 2.1, below. Thereafter, the remainder of this section will assist the contingency planners in:

- ☐ Identifying and defining their business functions;
- ☐ Applying criteria to assess business function criticality; and,
- ☐ Ranking critical business functions by their level of criticality.

Section Overview

- 2.1 Linking Day-to-Day Operations to the Mission**
- 2.2 Identifying and Defining Business Functions and Assessing Their Criticality**
 - 2.2.1 Isolating Critical Business Functions**
 - 2.2.2 Criteria for Assessing Business Function Criticality**
 - 2.2.3 Criticality Assessment**

2.1 Linking Day-to-Day Operations to the Mission

In general, each department or agency of the Federal government has an established mission. A mission is normally further broken down into measurable objectives that define specific macro-level actions that must be achieved by the Agency to accomplish its overall mission. Business programs and processes are established as the vehicles for accomplishing these objectives. See Figure 2.1.

Organizationally, the roles and responsibilities of the various components normally reflect their contribution to the achievement of one or more of the Agency's mission objectives. The day-to-day accomplishment of business

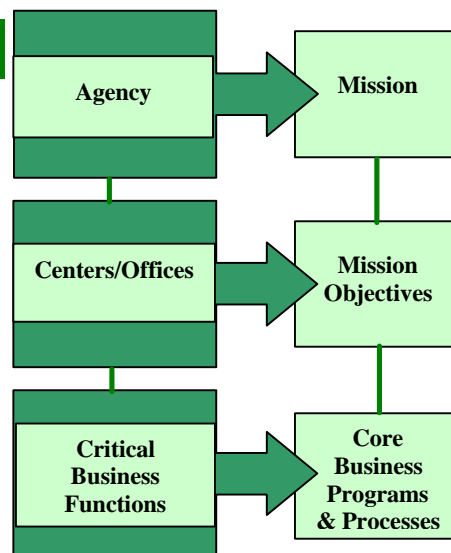


Figure 2.1

programs and processes is provided by each component's performance of its established business functions.

The *HCFA Enterprise Information Technology Architecture Report and Business Function Model (BFM)* define the overall mission of the Agency and identifies eleven core business areas.¹

- ☐ HCFA Management.
- ☐ Program Development.
- ☐ Program Operations Management.
- ☐ Medicare Financial Management.
- ☐ Program Integrity.
- ☐ Medicaid Administration.
- ☐ External Communication.
- ☐ Administrative Services.
- ☐ Beneficiary Outreach and Education.
- ☐ Health Industry Standards.
- ☐ Program Quality Management.

As mentioned before, the guiding principles for HCFA's Business Continuity Plan are to continue payment, safeguard the trust funds, protect quality care for its beneficiaries, and sustain beneficiary entitlement and enrollment. The contingency planners must be familiar with the guiding principles and the Business Function Model, and the processes operating within each of the eleven core business areas. The degree to which a business function supports one or more of these areas and the guiding principles should be considered in assessing its criticality.

2.2 Identifying and Defining Business Functions and Assessing Their Criticality

A *Business Function* is an activity that uses input in the performance of a given operation to produce output that supports the established business programs and processes. A business function may be performed by multiple components. A component may perform multiple business functions.

A business function has a clearly defined and unique purpose in a component's day-to-day operational activities. For example, a business function could be to provide for policy development and analysis, to support tracking of a program's execution (e.g., budget, schedule, etc), or to provide information essential to senior management decision-making.

A business function consists of three components: input, an operation which in some way processes this input, and an output generated by the operation. It is the output of a business function, and its value to the organization, that ultimately determines the function's criticality. Therefore, in the first step of the contingency planning process, the Agency's business functions must be identified and defined (through their inputs, processes and outputs) and then assessed as to their criticality in accomplishing the Agency's mission objectives.

¹ See HCFA Business Function Model for the detailed functions and processes for these eleven Function Areas.

The initial task of identifying and defining the Agency's business functions will be accomplished using Sections 1 and 2 of the Template. An individual report should be prepared for each identified business process. The contingency planners will use Section 1 to identify and define each of the office's business processes. They will use Section 2 to document the results of the process' criticality assessment.

2.2.1 Isolating Critical Business Functions

Using the Template each Workgroup should identify all business functions and their processes within the scope of its assigned business area. It should document the names and phone numbers of the Workgroup contact person and the lead component and the contact information for the business process. Further, after completion of the information, the completed analysis and assessment should be audited by at least one analyst familiar with the function, and reviewed by applicable management personnel. The "Reviewed by" field in each section records the name and phone number of the person who reviewed the section.

Items 1 to 15 of Template Section 1 describe a breakdown and analysis of the business area, function and process. They also record the components involved in the process, and functional interdependencies between processes. Further, for each of the function's outputs, these items identify the primary use of the output and an estimate of the "Maximum Acceptable Outage (MAO)" (i.e., the maximum amount of time that an output can be unavailable before operations are seriously impacted).

In completing items 1 to 15:

- ☐ The title of the business process under examination, and its corresponding business area and business function should be documented in the space provided.
- ☐ The "Description of the Process" should provide such information as:
 - the basic purpose of the process;
 - whether it is an automated or manual process;
 - a summary of what the process entails; and,
 - a summary of any interrelationship or interdependency shared with other operations within the Agency or outside agencies.
- ☐ Under "Interdependencies with Other Processes/Systems" list the titles of other business functions/processes that interface, in any way, with the one under study. Identify the relationship (e.g., the input to one process could be the output of another and vice versa; several functions/processes could share the same database and/or systems; outputs from both functions/processes may be necessary to fully support a core business program or process; etc).
- ☐ Next, describe the business process by way of its inputs and outputs, including:

- Identifying the type and source of each input. Input types may include hard copy reports, automated system updates, microfiche, E-mail, incoming phone calls, etc). An input source may be internal or external to overall Agency operations (e.g., data entry for information contained in an automated system may be accomplished by a Carrier). The type, location general size of the location (i.e., processing volume) of external input sites should be noted.
 - Describing the outputs of each process (e.g., reports, analyses, update of an automated system, etc). List all the outputs created by the process, the normal frequency of their production, and the time frame within which users require the output (e.g., end of month).
 - Noting the primary use of each output, including: the core business areas, programs and processes supported; and, the level within the business function/process that utilizes the output (e.g., Secretary, the business process users, etc).
- Based on the frequency that the output is produced, its purpose or primary use, the importance of the organizations/functions/processes using the output, time frames within which the output is needed, and the programs/activities supported, determine the maximum acceptable time that the output can be unavailable. The “Maximum Acceptable Outage (MAO)” is generally reported in hours or days.

Before providing guidance on Criticality Rating, we will first establish the criteria that will be used to assess business function criticality.

2.2.2 Criteria for Assessing Business Function Criticality

A Critical Business Function is a business function that directly supports HCFA in a core business area, program or process. The inability to perform a critical business function would adversely impact the accomplishment of mission objectives and prevent the Agency’s performance of its mission.

A business function’s criticality is based on the impact its loss would have on the accomplishment of overall mission objectives. The greater the impact; the higher the level of criticality. For the purposes of the current business contingency planning project, business processes will be assessed as either critical or non-critical. Those assessed to be critical will be further prioritized within the three levels of criticality defined below.

- **High Criticality – The loss of the business function would: prohibit the performance of the Agency’s core business areas, programs and/or processes; impede mission accomplishment; adversely impact existing working agreements with internal components and outside organizations; and jeopardize a business partner’s mission accomplishments.**

Examples of the conditions experienced in this category would include:

- A threat to the life or safety of individual beneficiary or groups of beneficiaries.

- A serious, negative impact on the Administrator's decision-making ability.
- An inability to accomplish essential Agency mission responsibilities (e.g., payment, program integrity, quality of care, and enrollment.)
- An inability to support key interfaces with essential operations and/or programs within other agencies' operations (e.g., Provider's core business).

- ❑ **Medium Criticality** – The loss of the business function would adversely impact Agency internal operations to the extent that: the ability to support core business areas, programs and/or processes would be seriously impaired; mission accomplishment would be jeopardized; and relationships with business partners would be strained.

Examples of the conditions experienced in this category would include:

- A serious, negative impact on the Agency's senior management's decision-making ability.
- An inability to manage key Agency programs.
- An impairment of management support and logistical activities (e.g., inability to process payroll, payment of commercial billings, procurement actions, transportation requests, etc).
- Impaired inventory control and accountability.
- Impaired legislative and/or regulatory capabilities.

- ❑ **Low Criticality** – The loss of the business function would adversely impact the day-to-day operations of the Agency and could, over time, degrade support to core business areas, programs and/or processes.

Examples of the conditions experienced in this category would include:

- An inability to request, or track the status of, facility work requests and projects.
- Incapacitated software security monitoring.
- Impaired supply issuance and control procedures.
- Impaired property accountability and tracking.

- ❑ **Non-Critical** – The loss or outage of the business function impacts the day-to-day operations of the Agency. However, support of core areas, programs and/or processes would not be impaired, and affected operations can functionally cope with the reduced capabilities.

Examples of the conditions experienced in this category would include:

- Lost capabilities affecting only minor systems, which are not essential to efficiently managing key programs and activities.
- Unimpaired management decision-making.
- Unimpaired inter-component/agency activities.
- Unimpaired accountability and control of essential resources.
- Backlogs or delays resulting from the loss of the business function(s) which are minor, do not significantly impair performance, and/or can be recovered effectively and efficiently when normal operations are restored.

2.2.3 Criticality Assessment

The criticality rating is accomplished by applying the criticality criteria provided above to item 16. Review the information up to item 15 to determine:

- ☐ The potential threat to human life and limb.
- ☐ The impact to four guiding principles: to continue payment, to safeguard the Trust Funds, to protect the quality of care for beneficiaries, and to sustain beneficiary entitlement and enrollment.
- ☐ The core business areas, programs and/or processes affected and the degree of impact.
- ☐ The management-levels within the Agency that will be affected and to what degree.
- ☐ The extent of any impairment of management's decision-making capability and the management levels effected.
- ☐ The existence and extent of any impact on business partner's operations.
- ☐ The extent of any potential economic impacts.
- ☐ The ability to maintain control and oversight of essential resources.
- ☐ The effect on day-to-day logistical and support activities.

Summarize the results of this review in item 17 "Rationale for Rating." Compare the results to the criteria outlined in Section 2.2.2 above, determine the applicable criticality-rating, circle the selected rating in item 16, and include the rationale for the rating in item 17.

Only the critical business functions will be considered in the remaining steps of the business continuity planning process.

Step 2:

Analyze and Document Resources and External Factors

3.0 SECTION INTRODUCTION

As noted in Section 1.0 to this handbook, contingencies may be caused by change of the inputs, threats from external events, and availability or usability of the resources used by critical business functions to accomplish their mission objectives. Therefore, to develop an effective business continuity plan for a critical business function we must identify the inputs, external events, and resources that it is dependent upon, and determine the extent of its dependency on each. Although they are each unique, inputs, external events, and resources are treated as process dependencies in the Template. In other words, the term "dependencies" includes inputs, external events or resources.

Section Overview

3.1 Categories of Dependencies

3.2 Business Process Resource Dependencies

3.2.1 Identify Dependencies

3.2.2 Assess Level of Dependencies.

3.1 Categories of Dependencies

The operations of critical business functions depend on the eight basic categories listed in Section 3 of the Template. Business-process-oriented workgroups will only concentrate their dependency analysis on inputs, external events, and primary resources including: information applications, human resources and supporting document. The infrastructure-oriented workgroups, such as telecommunication workgroup, will concentrate on infrastructure related resources. The eight categories are:

- A. Input: This category includes electronic input and manual or paper input to a process. The focus is on the input changes, either in terms of erroneous contents or volume of input.
- B. External Events: This category includes political situation, legal situation, regulatory changes, policy related events, congressional inquiries, media inquiries, weather, and environment (e.g., earthquake). Although most business processes deal with certain external events as a part of its regular processing, unexpected and significant change of external events can impose threats to the normal processing of a business function.
- C. Primary Resource Category:
 - 1. **Information Applications** – This category includes automated applications and the data processed and maintained by these applications. It does not include networks, operating systems, or other items that are infrastructure related. The focus is on information applications that directly support business-related activities.

2. **Human Resources** – Human Resources would include the staffing normally used in the performance of the function including both in-house and contractor personnel. If the function consists of more than one position type, then the number of people required in each position should be determined.
3. **Supporting Documentation** – This includes manuals, papers, forms, reports, hard copy records, and microfiche.

D. Secondary Resource Category:

- 1 **Telecommunications** – For the purposes of business continuity planning, the area of telecommunications will be limited to the availability of voice and data communications.
- 2 **Automated Data Processing (ADP) Infrastructure** – This area includes client-servers, local area networks (LAN), operating systems, and general software applications that are not specifically designed to support a business unique activity (e.g., word processing software). It also includes all hardware components used by a critical business in day-to-day operations (e.g., PCs, printers, scanners, modems, etc).
- 3 **Physical Infrastructure** – This category includes facilities, furniture, non-ADP equipment, security services, and non-IT systems such as power, fire alarms, climate control, and elevators.

3.2 Business Process Resource Dependencies

As noted at the end of Section 2 of this Handbook, once critical business functions are identified all data collection and analyses performed during the remaining steps of the contingency planning process will be applicable to these functions/processes only. Therefore, Step 2 only requires identifying and assessing the resources required by each of the critical business functions identified in Step 1. This will be accomplished by completing Section 3 of the Template, which essentially deals with two key pieces of information: identifying the resources (inputs, external events, and resources) and determining resource dependencies.

3.2.1 Identifying Dependencies

The first step is to identify the input and resources used by the critical business function and external events that may affect the operations, *during the course of **normal** operations*. The types of information noted below should be included for the basic dependency categories. Wherever possible, quantify the dependencies **in normal operations**.

- ☐ **Input** -- Identify the various types of input that feed to the business operation and their regular volume.

- ☐ **External Event** – Identify the potential external events caused by Year 2000 problems that may affect the business process.
- ☐ **Information Applications** – List the applications used by the critical business function and identify the Criticality Level assigned to each application assessed in the Year 2000 Renovation Program. Summarize the purpose of each application and the type of data used in each.
- ☐ **Human Resources** – Identify the various types of positions, the number of personnel assigned to each type of positions, and a description of the work performed by each position.
- ☐ **Supporting Documentation** – List the documentation normally used in day-to-day operations (e.g., forms, hard copy records) and those that may be referred to periodically (e.g., manuals).
- ☐ **Telecommunications** -- Identify the telecommunication needed to perform the critical business function. For example: estimate the capacity and geographical coverage provided by the telecommunication.
- ☐ **ADP Infrastructure** – Identify the ADP infrastructure hardware and software used by the critical business function. List hardware components by type (e.g., PCs, printers, scanners, etc) and indicate the number of each normally used. Also, identify the software used by name (e.g., WordPerfect, Microsoft Word, Lotus 1-2-3, etc).
- ☐ **Physical Infrastructure** – Identify the physical resources normally needed to perform the critical business function. For example: estimate the amount of square footage assigned to the function, identify non-ADP equipment by type and number, indicate the number of telephone instruments normally used and any special telecommunication requirements (e.g., fax, voice mail), note any special security requirements, and identify special requirements associated with the physical infrastructure required (e.g., elevators for handicapped employees)

3.2.2 Assessing the Level of Dependencies

Once the various dependencies are identified, the workgroup will assess the critical business function's level of dependency on each of the identified inputs, external events, and resources. The degree of dependency should be ranked as low, medium or high as defined below:

- A. For Input the level of dependency is based on how much the business process relies on the normal flow of the input:

- ☐ **Low** – Inputs that are occasionally used in day-to-day operations, but are not essential to actually accomplishing the critical business function's requirements. Hence, changes in the content or volume will NOT affect the business function.
- ☐ **Medium** – Inputs that are used during the normal course of critical business function operations, but whose immediate availability is not essential. Or, changes in the content or volume of the input will somehow affect accomplishing the critical business function.
- ☐ **High** – Inputs which are used frequently in day-to-day operations and are essential to the proper accomplishment of critical business functional requirements. Or changes in the contents or volume of the input will significantly affect accomplishing the critical business function.

B. For External Events:

- ☐ **Low** – Events that occasionally affect day-to-day operations, and impose no or insignificant threat to accomplish the critical business function.
- ☐ **Medium** – Events that impose some threat to accomplish the critical business function.
- ☐ **High** – Events that impose significant threat to accomplish the critical business function.

C. For Resources:

- ☐ **Low** – Resources, which are occasionally used in day-to-day operations, but are not essential to actually accomplishing the critical business function's requirements. Examples may include:
 - A secretarial position that provides general administrative support, but is not directly involved in the tasks performed to accomplish the critical business function;
 - An automated system that was ranked as non-critical during Y2k program planning;
 - Network connectivity is not essential since the function utilizes a stand-alone PC and software (but, if information used by the function is often exchanged using E-mail the dependency may be higher);
 - Telephones that are used only for general communications and not directly in support of the function; and,
 - Manuals that are not frequently used in critical business function operations.
- ☐ **Medium** – Resources that are used during the normal course of critical business function operations, but whose immediate availability is not essential. Examples may include:
 - A position primarily used only in the preparation of month end reports;

- An automated system that was ranked at Critical Level II and III during Y2k program planning;
 - A printer required only in the preparation of month-end reports;
 - A fax machine used only in the distribution of month end reports; and,
 - Hard copy records used only during the review of month-end reports.
- **High** – Resources that are used frequently in day-to-day operations and are essential to the proper accomplishment of critical business function requirements. Examples may include:
- A position responsible for entering a large volume of data in a database;
 - Automated systems ranked at Critical Levels I during Y2k program planning;
 - PCs used in daily operations;
 - Telephones or data communications used to collect information used in operations; and,
 - Records used to accomplish key analyses.

In the case of quantifiable resources, include the minimum number or quantity of each resource required to effectively support the critical business function in a contingency situation.

Step 3:

Establish and Document Risk Conditions

4.0 SECTION INTRODUCTION

To develop an effective contingency plan, contingency planners must determine how resources will be impacted. To accomplish this, risk conditions are developed to: identify contingencies that may occur, define resulting conditions, and assess the effect on inputs, external events and resources. The business process workgroups will consider the following resources in developing risk conditions:

- ☐ IT Applications;
- ☐ Human Resources; and,
- ☐ Supporting Documentation.

Section Overview

- 4.1 Agency-Wide Risk Scenarios and Policy**
- 4.2 Establish Relationship Between Agency-Wide Scenarios and Workgroup Risk Conditions**
- 4.3 Recording the Risk Conditions in Section 4, Risk Identification and Assessment**

The infrastructure workgroups will consider the following resources in developing risk conditions:

- ☐ Telecommunications (*Voice and Data Communications*);
- ☐ ADP Infrastructure (*WAN, LAN, Hardware, Operating Systems, Standard Office Software*); and,
- ☐ Physical Infrastructure (*Facilities, Non-ADP Equipment, Supporting Services and Non-IT Systems*).

4.1 Agency-Wide Risk Scenarios and Policy

The Scenarios Development and Policy Analysis Team will identify Agency-wide scenarios based on the overall Medicare and Medicaid structure for the beneficiaries. These scenarios cover macro-level problems in the areas of: Medicare processing failure, Medicaid processing failure, Provider systems failure, Infrastructure failure, Carrier and Intermediary systems failure, Standard system failure, etc. This team will generate two types of scenarios: 1) business-oriented scenarios (e.g., claims cannot be processed), and 2) dependency-oriented scenarios (e.g., telecommunication is not available). This team will also define policy and strategy for each of the scenarios. The policy and strategy will be reviewed by the Executive Council for approval. The strategy and policy for the scenarios will guide the workgroups to determine alternate strategy for each risk condition that are related to the agency-wide scenarios.

Dependency related scenarios may be combined to anticipate the compound effect of the situation. One possible combination may be like the following:

- ❑ **IT applications are Unusable** - All information applications, critical and non-critical, are lost due to: the post-implementation failure of, or delays in renovation and testing, these systems; and/or the inability to interface with, and obtain essential data from, the information systems of partner agencies and departments (e.g., the Federal Reserve or the Department of Health and Human Services).
- ❑ **IT Applications & Telecommunications are Unusable** - Same conditions as in #1 above, plus voice and data telecommunications (including LAN and WAN *connectivity*) are lost due to problems with circuits, switching systems, network connections, etc. ADP hardware, operating systems, standard office software operate in a stand-alone mode only.
- ❑ **IT Applications, Telecommunications and ADP Infrastructure are Unusable** - Same conditions as in the previous two examples, above, plus ADP hardware, operating systems, and standard office software become inoperable due to Y2k non-compliance. Network and stand-alone operability are lost.
- ❑ **IT Applications, Telecommunications, ADP Infrastructure and Physical Infrastructure are Unusable** - Same conditions as in the previous three examples, above, plus facilities, non-ADP equipment and Non-IT systems are unusable.

4.2 Establish Relationship Between Agency-Wide Scenarios and Workgroup Risk Conditions

The next step is to identify, for each critical business process, the specific dependencies that would be affected under each macro-level dependency scenario. (The process dependencies in Section 3 of the Template). Further, the risk condition should detail how the dependencies might be affected, since this information could have implications on potential continuity planning approaches. For example, in the case of IT systems, dependencies on system interfaces with other systems both within and outside of the Workgroup's operations, and the impact of their loss, should be identified.

In developing risk conditions, the contingency planners should adhere to several contingency planning "rules of thumb".

- ❑ **Determine vulnerabilities and then plan for a "worst case" risk condition.** Basically, planning activities do not have to plan for every imaginable threat, only those where a significant risk potential exists. However, once vulnerability to a threat has been established, scenarios developed to characterize its potential impact should define the "worst case" conditions.
- ❑ **Risk conditions should focus on problems not symptoms.** A single problem may have many symptoms. Actions incorporated in contingency plans must focus on overcoming problems that constrain or prevent the performance of a critical business

function. When the core problem is resolved so are the symptoms associated with the problem.

- ❑ Risk conditions should be properly targeted to the planning activity. Risk conditions must be specifically geared to the problem facing the applicable planning activity. If this is not done, planners may waste time and complicate the planning process by addressing issues that are more symptomatic and not focused specifically on the problem directly affecting them. For example, water and power outages are potential contingencies that must be planned for by Facility Management. Because the Workgroup cannot restore water or power, planning for these conditions should focus on the loss of facility space and the potential need to relocate, rather on restoring water or power.

4.3 Risk Identification and Assessment

Risk conditions are used as input to the Business Impact Analysis (BIA), Step 4 of the contingency planning process. These risk conditions are documented and utilized in the analysis by recording them in Section 4 of the Template. The Workgroup risk conditions recorded in the first part of section 4 of the template should provide both the name and a narrative description of the risk condition.

- ❑ The risk name is a brief, descriptive statement (one or two lines) which emphasizes or summarizes the conditions of the scenario. It will be used to link future steps in the business continuity planning process (e.g., the development of alternate strategies) back to the scenarios and BIA.
- ❑ The risk condition should also be defined in sufficient detail to fully understand the resources affected and the manner in which they are affected.
- ❑ For each business process, there may be multiple risk conditions. As the risk condition build with the addition of each new element, it is not necessary to re-state the conditions from the preceding one. Simply state that the conditions in the preceding section apply (note any exceptions), and define the adverse conditions posed by the addition of new constraining elements.

Step 4:

Perform and Document Business Impact Analysis

5.0 SECTION INTRODUCTION

In the last step, we determined the effect of the assumed risk conditions on the resources supporting each of the identified critical business process. In this step, we carry the analysis forward to determine the resulting operational impacts on each critical business process.

Section Overview

5.1 Focus of the Business Impact Analysis

5.2 Risk Identification and Assessment

5.1 Focus of the Business Impact Analysis

As noted above, the focus of the Business Impact Analysis is on the anticipated operational impacts that an established risk condition would have on the critical business process. To assist in this analysis, planners should review the forms completed up to this point in the process for each of the critical business processes. Some of the questions that should be specifically addressed in performing the analysis include:

- ☐ How will the constraints placed on the dependencies affect the processes and outputs of the critical business process? What will and will not be available? What can and cannot be accomplished?
- ☐ Are there operational interfaces between the critical business process being reviewed and other business processes internal and external to the component(s)? If so, how will they be affected by the contingency? What will and will not be available? What can and cannot be accomplished?
- ☐ What offices, programs, and/or external departments and agencies, if any, will be affected by the risk condition? How will problems in these activities affect the critical business process?
- ☐ How will support normally provided to the above activities be affected? What will be the ramifications?
- ☐ How will the overall effects, established above, change when the risk condition lasts longer? (**Note:** For purposes of this effort, the effects of a risk condition will be viewed over a short- (7 days or less), medium- (8 to 30 days), and long-term (more than 30 days) duration).

5.2 Risk Identification and Assessment

A Business Impact Analysis will be performed for each of the risk conditions recorded in the first part of Section 4 of the Template. The questions listed above should be used as a starting point in performing the analyses. Each analysis should be specific in defining what is affected,

how it is affected, what will not be available or accomplished, who and what will be impacted. Figure 5.1 provides a simple example of the process used to assess the business impacts.

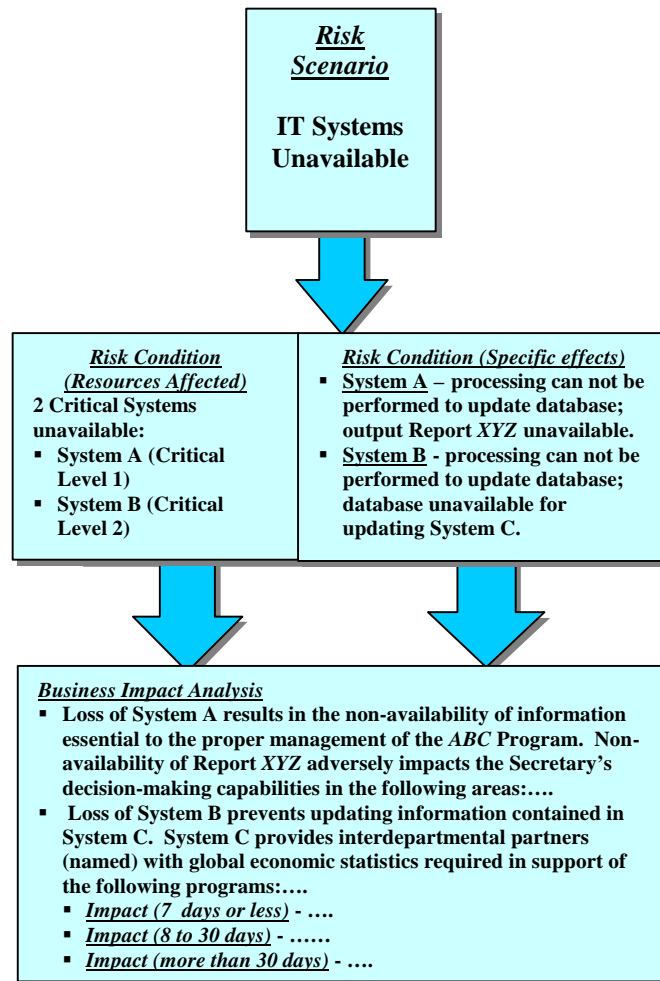


Figure 5.1

The information shown in the Business Impact Analysis block at the bottom of Figure 5-1 is the basic type of information that should be reflected in the affected outputs and/or functions and affected users and/or entities part for each of the risk condition.

Then, the contingency planners should analyze the probability of occurrence for each of the risk conditions. The probability may be estimated quantitatively or qualitatively. It will be marked as:

1. Certain if the probability is between 90% and 100%,
2. Probable if the probability is between 50% and 90%,
3. Possible if the probability is between 10% and 50%,
4. Improbable if the probability is between 0% and 10%.

The workgroup should also analyze the impact on business impact if the risk condition occurs. The impact will be marked as:

1. Catastrophic if it will cause total failure or serious degradation in core function
2. High if it will impair the performance or potential political embarrassment,
3. Moderate if it will cause some noticeable impact on some sector of operations,
4. Low if it has very little effect.

Based on the probability of the risk condition and its business impact, contingency planners will preliminarily determine whether a risk condition requires a Risk Mitigation Plan (RM) and a Contingency Plan (CP), only a Contingency Plan, a Contingency Plan or a Risk Mitigation Plan, or watching the situation. The proposed risk responses will be grouped and recommended to the Executive Council. The Executive Council will review and determine the response. The following table lists these proposed responses to the risk conditions.

Impact Probability	Catastrophic	High	Moderate	Low
Certain	RM and CP	RM and CP	CP	RM or CP
Probable	RM and CP	RM and CP	RM or CP	Watch
Possible	CP	CP	RM or CP	Watch
Improbable	CP	RM or CP	Watch	Watch

For the risk conditions that need Risk Mitigation Plans, the DACP team will track the risk mitigation activity through information provided in Section 5 of the Template. It tracks, risk mitigation plan summary, actions to date, criteria for evaluating mitigation status, and current mitigation status (red, yellow, or green).

Step 5:

Develop, Evaluate, and Document Contingency Strategies

6.0 SECTION INTRODUCTION

The Business Impact Analysis performed in Step 4 provides the foundation upon which Step 5 is based. By this point in the business continuity planning process, the Workgroups have identified the components' critical business functions and processes, determined the resources used by each, and assessed the impact of various risk conditions on those resources. In this step, the Workgroups identify logical process groupings for contingency planning and identify, evaluate, and document alternate strategies Contingency Plan and Risk Mitigation Plan strategies.

Section Overview

- 6.1 Identifying Logical Process Groupings for Contingency Planning**
- 6.2 Developing Potential Alternate Strategies**
- 6.3 Evaluating, Documenting, and Selecting Alternate Strategies**

6.1 Identifying Logical Process Groupings for Contingency Planning

Initially, in Step 5, contingency planners analyze the processes identified in the Business Impact Analysis to determine logical process groupings for subsequent contingency planning. Some possible strategies might include:

1. Grouping multiple processes together.
2. Grouping similar risk conditions, resources, and triggers.
3. Subdividing processes (separate risks may need different plans).
4. Including processes assigned to other components or workgroups (need cross-component coordination).

6.2 Developing Potential Alternate Strategies

The next step is to develop alternative strategies to continue critical business function processes despite the non-availability of a dependency or the failure of a process (e.g., using manual procedures to process data when automated processes are not operational, downloading and processing data on a stand alone PC and software when networks are unavailable, etc). *See Figure 6.1, below.* If any of the processes have pre-existing contingency plans they should be documented at this stage as a starting point for reviewing their currency.

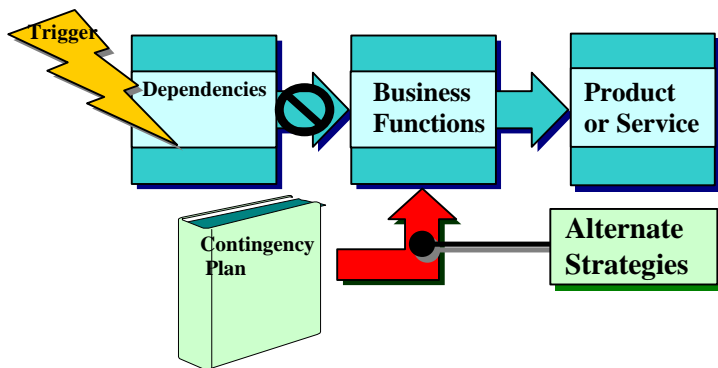


Figure 6.1

Developing alternate strategies is a creative process that consists of:

- ☐ Breaking down and analyzing the key components of each identified risk condition.
- ☐ Doing a “side-by-side” comparison of the risk conditions and the processes performed in accomplishing a critical business function to determine where the risk conditions may interject problems or stopgaps in the normal flow of each process. *See Figure 6.2, right.*
- ☐ Developing alternate strategies that utilize one or more of the following methods:

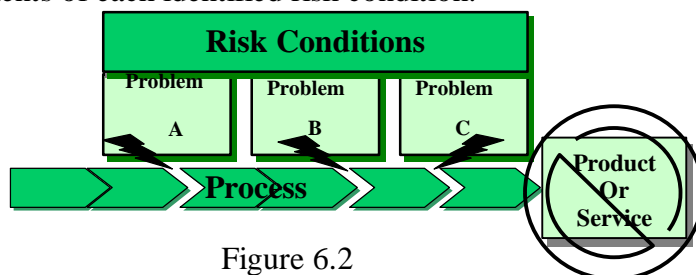


Figure 6.2

1. Identification of alternative resources to replace or strengthen unavailable or impaired resources, which support critical business functions. In this step, Workgroups identify alternate resources or inputs to reduce the impact of impaired or unavailable dependencies (e.g., contractor support to cover for the non-availability of assigned personnel or to help cover increased workload, cellular phones to substitute for lost land-lines, etc).
2. Identification of "work-arounds" to circumvent portions of impaired processes at the anticipated point(s) of failure;
3. Identification of "patches" to bridge portions of impaired processes at the anticipated point(s) of failure; and,
4. Identification of a new alternate process which produces an acceptable product or service in support of the critical business function and is less susceptible to points of failure than the existing process.

The Workgroups should initiate a "brainstorming session" in which alternate strategies are suggested without assessing their strengths and weaknesses. Where components or workgroups share related processes, brainstorming should include stakeholders from each of the components or workgroups.

The brainstorming session should:

- Define the contingency plan objectives;

- Define the minimum acceptable level of service;
- Include policy-makers as well as business and system analysts; and,
- Generate options.

The following generic process of commuting to work illustrates the brainstorming task. If a Business Impact Analysis were completed for regarding commuting to work, many individuals would likely identify their automobile as a dependency. If a person's automobile were to fail to start one morning some alternate strategies for commuting to work might be:

1. Repairing the automobile.
2. Purchasing a new automobile.
3. Borrowing an automobile.
4. Asking a friend to provide a ride to work.
5. Carpooling with a colleague.
6. Taking a taxicab to work.
7. Taking a bus to work.
8. Taking a bicycle to work.
9. Working from home.

These are the more traditional responses. However, during the brainstorming session considering non-conventional alternatives should be encouraged (i.e., thinking "outside of the box"). Doing so might yield the following additional potential strategies:

1. Taking a boat to work.
2. Hang-gliding to work.
3. Taking a plane and parachuting to work.
4. Finding a new job which is within walking distance of home.

There is no standard set of alternate strategies that can be applied in all situations, and strategies that work in one situation may have to be tailored to work in another. The following are a few examples of some basic strategies that can be expanded upon, modified, and/or combined to overcome risk conditions.

- ☐ Using contractor support to handle personnel shortages or increased workload
- ☐ Use remote disaster recovery site. This may include arranging alternate recovery site, assembling and maintaining a package of required materials for the alternate site (e.g., supplies, forms, records, etc).
- ☐ Use alternate/backup systems, applications, networks. This may include downloading databases and applications to a local, standalone PC and processing data offline to offset the loss of the network; using off the shelf software to substitute for standard applications; leasing back-up equipment; or processing data offline to offset the loss of the network.
- ☐ Reduce dependencies on telecommunications and network connectivity. This may include data processing on a standalone platform or centralized area or by identifying tasks that can be accomplished by personnel working at home.
- ☐ Performing processes prior to 12/31/1999 if possible.

- ❑ Manual processing.

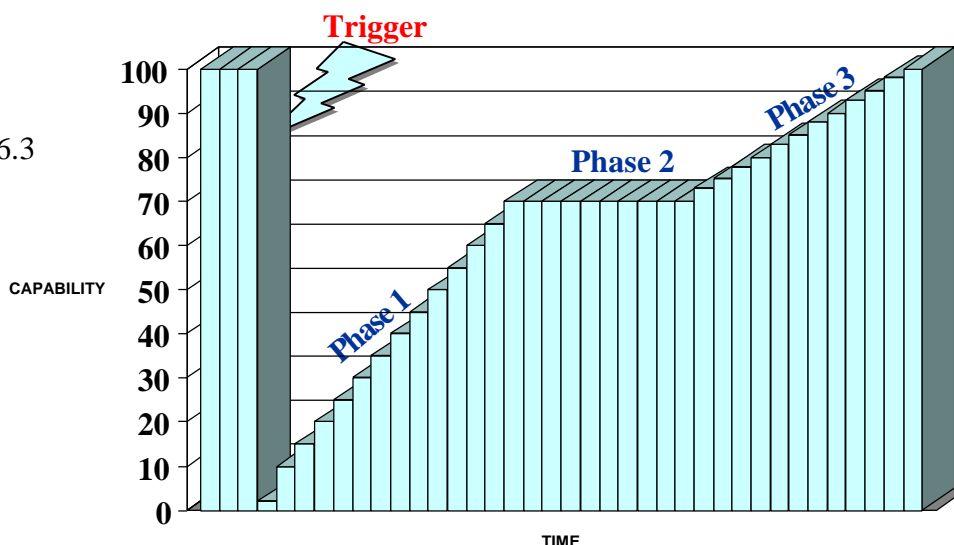
Alternate strategies should be developed for each of the three phases of contingency operations, illustrated below in *Figure 6.3*.

Phase 1 Recovering Critical Business Functions – Planning actions are focused on the immediate response to the disruption, and the initiation of pre-planned activities (e.g., implementing manual procedures) which provide the component(s) with the capability to perform critical business functions at a pre-determined degree of capability and level of productivity. A goal of contingency planning at this stage is to recover the ability to perform critical business functions as quickly as possible.

Phase 2 Maintaining Continuity – Planning actions support the review, analysis and (if necessary) adjustment of continuity operations to ensure that critical business functions are being performed within the planned degree of capability/productivity (e.g., assessing the accuracy of the data being recorded; ensuring that any processing backlogs are not greater than planned).

Phase 3 Restoring Normal Operations – Planning actions focus on transitioning from the continuity level of operations to the full restoration of normal operations, when conditions permit (e.g., recording data in critical automated systems, once they become available, to bring them up to date).

Figure 6.3



6.3 Evaluating, Documenting, and Selecting Alternate Strategies

Once the brainstorming is completed, the list of potential alternate strategies should be analyzed. The Template has been developed to assist in this analysis. This consists of the following steps:

1. Reviewing and discussing the list of potential options to assess the implementation and funding requirements against anticipated benefits.
2. Eliminating the weaker approaches.
3. Combining options if doing so will offset weaknesses in the individual approaches and will provide for a stronger overall strategy.
4. Listing remaining strategy options.
5. Listing the resources that would have to be procured and/or assembled to implement each strategy (e.g., a standalone PC, cellular phones, off-the-shelf software, contractor support, back-up equipment, etc).
6. Developing cost estimates to implement each alternate strategy.
7. Obtaining clearances from Security, Privacy, Legal, and Program Integrity components.
8. Preparing and transmitting to the Executive Council, decision memoranda, which document the alternatives, evaluates the alternatives, recommends one or more proposed alternate strategies, and recommends Emergency Response Team (ERT) members to complete and execute the contingency plans.

The Executive Council will review the decision memoranda, will determine which alternate strategies will be implemented, and will determine the composition of the ERT.

Step 6, Part 1:

Draft Conntingency Plans

7.0 SECTION INTRODUCTION

The forms and information collected and analyzed during the first five steps of the contingency planning process should be maintained in folders, by critical business function. In preparing to write a contingency plan, the contingency planners should review this documentation to re-familiarize themselves with the information collected. Next, prior to drafting the formal plan, the contingency planners should develop an outline of the processes and procedures that would have to be accomplished to execute the alternate continuity strategies developed in Step 5 of the process.

Section Overview

- 7.1 Developing a Project Plan**
- 7.2 Developing Plan Processes and Procedures**
- 7.3 Drafting the Contingency Plan**
- 7.3 Developing and Documenting Contingency Plan Administrative Procedures**

7.1 Developing a Project Plan

Once the Executive Council has approved the alternate strategy and has designated the staff and lead component of the ERT, the ERT should be assembled. Within three weeks of the Executive Council's approval of the contingency strategy, each ERT must prepare a project plan and deliver the plan to the DACP, through the ERT's Support Team contact. The project plan should list the actions that must take place in order to complete documentation of the contingency plan, when these actions will commence, when they will conclude, and who is responsible for completing each action item. The following is an example:

Project Plan

For each task, identify beginning and ending dates and person(s) responsible:

1. Prepare recall roster to permit speedy contact and assembly of key personnel.
2. Establish what metric will be necessary to determine trigger is met and establish reporting system if the metric is not currently available.
3. Prepare procedures for monitoring status of potential triggers and for reporting conditions to higher authority.

4. Prepare operating instructions for carriers, Fis, regional offices, etc.
5. Prepare procedures for communicating with external business partners (e.g., contractors) during contingencies
6. Prepare procurement/purchase order.
7. Train Staff.

Project plans are to be updated every two weeks and provided to the DACP through the ERT's Support Team contact.

7.2 Developing Plan Processes and Procedures

After the project plan has been drafted, the ERT should develop and draft the contingency plan processes and procedures. The alternate strategies developed by the Workgroup should be analyzed to determine the major tasks and activities that would have to be performed, in a contingency situation, to execute each strategy. These tasks and activities, when viewed in order of their performance, become the basis for the processes and procedures that will be initiated immediately following the occurrence of a contingency, and used to recover critical business functions, maintain continuity, and eventually restore normal operations.

The contingency planners should first develop a summary outline of these processes and procedures to use as a guide in drafting the contingency plan. The Template will be used to develop and document this outline.

The Template should be completed for each of the alternate continuity strategies to be used by the Workgroup. Each alternate continuity strategy should be analyzed and broken down into the major tasks and supporting activities that would be accomplished in its execution. These tasks and activities should cover the three phases of the recovery process, covered earlier in Section 6.2, as follows:

- ☐ **Recovering Critical Business Function:** Record the steps, relevant to the applicable strategy, which would be accomplished to recover the critical business function immediately following a contingency. These are all the tasks and activities required to overcome the identified disruptions to operations and establish business continuity.
- ☐ **Maintaining Continuity:** Record any tasks and activities that must be accomplished, over the course of a contingency, to sustain the established level of business continuity. Any duration-sensitive considerations identified in the Business Impact Analysis and covered in strategy development, should be planned for at this point.

- ❑ **Restoring Normal Operations:** This section covers the actions that would be taken to handle a return to normal operations after the adverse conditions resulting from the contingency have been corrected. For example, the restoration of critical IT systems would require the identification of data not recorded in the system, due to the contingency, and entry of the data to bring the system up to date.

Individual sections have been provided on the Template to organize the actions applicable to each phase. Care should be taken to record the information sequentially (i.e., in the logical order in which they would be accomplished) in each of the three sections of the form. Task and activities should be recorded in short but descriptive statements.

7.3 Drafting the Contingency Plan

Once outlining of the contingency plan processes and procedures has been completed, the drafting of a formal contingency plan can be accomplished. The outline for a contingency plan appears in Appendix D of this Handbook. The information previously recorded in Section 5 of the Template should be transferred to the contingency plan.

7.4 Developing and Documenting Contingency Plan Administrative Procedures

Each ERT must develop internal contingency plan administrative procedures that will be later documented in their contingency plan. These procedures should include such requirements as the following:

- ❑ A recall roster to permit speedy contact and assembly of key personnel.
- ❑ Staffing and operating procedures for an Emergency Response Team (ERT) to be accountable for executing the contingency plan.
- ❑ Checklists to support timely implementation of contingency plan processes and procedures.
- ❑ Procedures for requesting additional resources and requirements identified during actual contingency conditions.
- ❑ Procedures needed to monitor status and report conditions to higher authority.
- ❑ Procedures for communicating with other ERT for other processes and external business partners during contingencies.

Steps 5 & 6:

Plan Risk Mitigation and Mitigate Risks

8.0 SECTION INTRODUCTION

Although it would be reassuring to completely eliminate all risks, which an organization may face, oftentimes this is not possible. Even in those instances where eliminating a risk is possible, the benefits of eliminating a risk, as opposed to reducing the risk to an acceptable level, sometimes do not outweigh the cost required to do so. Risk mitigation planning acknowledges such competing objectives and therefore, the purpose of risk mitigation planning is to reduce, to an acceptable level, the likelihood that a specific risk will threaten operations.

Section Overview

- 8.1 Establishing Risk Mitigation Timeline**
- 8.2 Developing Potential Alternate Strategies**
- 8.3 Evaluating, Documenting, and Selecting Alternate Strategies**
- 8.4 Implementing the Risk Mitigation Plan**

8.1 Establishing Risk Mitigation Timelines

As a result of the Business Impact Analysis, pertinent risk conditions have been identified and the probability of occurrence and estimated impact of each risk condition have been evaluated. If the result of the probability and estimated impact indicated the need to establish a risk mitigation plan, then the next planning step is to establish timelines for specific actions to mitigate the identified risk conditions. This includes:

- Documenting the objectives of the risk mitigation plan.
- Identifying the Event Horizon Date/Time Horizon To Failure. This is the date when the risk condition is likely to threaten the organization. For example, January 1, 2000 would be one Year 2000 Event Horizon Date.
- Establishing drop dead renovation/remediation completion dates. These are dates which should precede the Event Horizon Date, in order to permit testing to evaluate the success of the renovation/remediation efforts.
- Determining the lead time required to complete risk mitigation.

8.2 Developing Potential Alternate Strategies

The process for “Developing Potential Alternate Strategies” for risk mitigation plans is similar to the process stated earlier in Section 6.1.2, regarding contingency plans. The contingency planners should initiate a “brainstorming session” in which alternate strategies are suggested without assessing their strengths and weaknesses. Where components or workgroups share related processes, brainstorming should include stakeholders from each of the components or workgroups.

The same generic process of commuting to work which was stated earlier to illustrate the concept of “brainstorming” in developing contingency plans can be referred to here in order to illustrate the differences in brainstorming in developing risk mitigation plans. A Business Impact Analysis which was completed for the function of commuting to work, for many individuals would likely identify the automobile as a dependency, and automobile failure as a risk condition. This is the same in both contingency plan development and in risk mitigation plan development.

The differences occur in the timing of the strategy relative to the risk condition’s Event Horizon Date. The potential alternate strategies involved in contingency plans focuses on continuing critical functions after the Event Horizon Date has occurred. In other words, strategies such as repairing the automobile, carpooling, or taking a taxicab to work, each focus on getting to work after the car has failed to run.

The focus of risk mitigation plans, on the other hand, is on preventing the risk condition from occurring, or in other words, upon activities occurring prior to the Event Horizon Date. Strategies such as preventative maintenance (i.e., checking the tires to make sure they are properly inflated, checking the engine fluid levels to make sure they are full and clean, replacing all worn engine parts, etc.) which focus on reducing the likelihood that the car will fail to run, prior to the car's failure to run, are examples of risk mitigation strategies.

During the brainstorming session considering non-conventional alternatives should be encouraged (i.e., thinking “outside of the box”). There is no standard set of alternate strategies that can be applied in all situations, and strategies that work in one situation may have to be tailored to work in another. The following are a few examples of some basic risk mitigation strategies:

- ☐ Building bridges for non-compliant interfaces; and;
- ☐ Using alternate systems, applications, and/or networks.

If it is determined that it would be advantageous to conduct business differently than is documented in the risk mitigation plan, after the threat of the risk condition occurring has passed (i.e., returning to normal operations, transitioning to new operations, etc.), then the risk mitigation plan should include information on how this restoration or transition is to occur upon termination of the risk mitigation operations.

8.3 Evaluating, Documenting, and Selecting Alternate Strategies

Once the brainstorming is completed, the list of potential alternate strategies should be analyzed. This consists of the following steps:

1. Reviewing and discussing the list of potential options to assess the implementation and funding requirements against anticipated benefits.
2. Eliminating the weaker approaches.
3. Combining options if doing so will offset weaknesses in the individual approaches and will provide for a stronger overall strategy.
4. Listing remaining strategy options.
5. Listing the resources that would have to be procured and/or assembled to implement each strategy (e.g., a standalone PC, cellular phones, off-the-shelf software, contractor support, back-up equipment, etc).
6. Develop cost estimates to implement the strategy, using the Costing Worksheets for Y2K Risk Mitigation and Contingency Plans (Appendix C).
7. Obtaining clearances from Security, Privacy, Legal, and Program Integrity components.
8. Preparing Decision Memoranda to the Executive Council, which documents the alternatives, evaluate the alternatives, and recommends one or more proposed alternatives.

The Executive Council will review the Decision Memoranda and will determine which alternate strategies will be implemented.

Once the Executive Council has approved the Risk Mitigation Strategy, the Risk Mitigation Planners should document the Risk Mitigation Plan, by using the Risk Mitigation Plan Outline (Appendix E), and by referring to the information recorded in Section 6 of the Template.

8.4 Implementing the Risk Mitigation Plan

The risk mitigation strategy selected in Step 5 must now be executed in Step 6. This requires the component to monitor the condition of resources to determine the execution of the risk mitigation plan. Additionally, the implementation of the risk mitigation plan may also require the component(s) to establish support agreements with vendors that provide the following alternative solutions: networking, developers and maintainers, or computing centers.

Once the risk mitigation plan has been implemented, there may come a time when it is determined to be advantageous to restore operations to their previous configuration. Therefore, risk mitigation plans should include plans to return to normal operations once the threat of the risk conditions occurring has passed.

Appendix A

Glossary

Alternate Continuity Strategy - An approach for accomplishing a critical business function in the event that change of inputs, threats from external events, and/or loss of supporting resources prevents an organization from accomplishing its critical business functions through normal operations.

Alternate Site - A location, other than the main facility, which can be used to conduct business functions.

Application - A computer program designed to help people perform a certain type of work. Depending on the work for which was designed, an application can manipulate text, numbers, graphics, or a combination of these elements.

Architecture - A description of all functional activities to be performed to achieve the desired mission, the system elements needed to perform the functions, and the designation of performance levels of those system elements. An architecture also includes information on the technologies, interfaces, and location of functions and is considered an evolving description of an approach to achieving a desired mission.

Auditing - A thorough examination and evaluation of plans and procedures to verify their correctness and currency.

Business Area - A grouping of business functions and processes focused on the production of specific outputs.

Business Continuity Plan - An approved set of arrangements and procedures which enable an organization to respond to threats in such a manner that the organization's critical business functions continue without interruption or essential change.

Business Continuity Planning - The process of developing advance arrangements and procedures in response to potential events, which could negatively impact an organization, in order to enable the organization to ensure continued performance of its critical business functions without interruption. Business Continuity Planning contains two parts: Risk Mitigation Planning (to reduce the likelihood that such events will occur) and Contingency Planning (to ensure the continued performance of critical business functions if the events do occur).

Business Function - A group of logically related tasks that are performed together to accomplish a mission-oriented objective.

Business Impact Analysis (BIA) - Analyzes the specific impacts of an established risk condition on the outputs of a critical business function and the resulting degradation of the function's ability to support core programs and processes.

Business Plan - An action plan that the enterprise will follow on a short-term and/or long-term basis. It specifies the strategic and tactical objectives of the enterprise over a period of time. The plan, therefore, will change over time. Although a business plan is usually written in a style unique to a specific enterprise, it should concisely describe “what” is planned, “why” it is planned, “when” it will be implemented, by “whom” it will be implemented, and “how” it will be assessed. The architects of the plan are typically the principals of the enterprise.

Business Process - The combination of inputs, resources, actions, and decision that produces output (or set of outputs) that support one or more business functions.

Cold Site - An alternate operating facility that is void of any resources or equipment except air conditioning and electrical wiring. Equipment and resources must be installed in such a facility to duplicate the critical business functions of an organization. Requires time for equipment delivery, installation, and testing. Cold sites have many variations depending on their communications facilities, UPS systems, and mobility. Also known as a shell site.

Command Operations Center (War Room) - A facility, which is separated from the main facility, with adequate communications equipment from which initial recovery efforts are manned and media-business communications are maintained. This facility is used temporarily by the management team to begin coordinating the recovery process and is used until the alternate sites are functional.

Component - A single resource with defined characteristics. The component concept is used in defining precise specifications for testing the validity of various resources. These components are also defined by their relationship to other components.

Configuration Management - The continuous control of changes made to a system’s hardware, software, and documentation throughout the development and operational life of the system.

Contingency - An event that is of possible but uncertain occurrence.

Contingency Plan - In the context of the Year 2000 program, a plan for responding to the loss or degradation of essential services due to a Year 2000 problem in an automated system. In general, a contingency plan describes the steps the enterprise would take, including the activation of manual or contract process, to ensure the continuity of its core business process in the event of a Year 2000 -induced system failure.

Contingency Planning - The process of developing advance arrangements and procedures which will enable an organization to respond to events that are of possible but uncertain occurrence.

Controls - Measures designed to reduce or eliminate threats.

Conversion - The process of making changes to databases or source code.

Criticality Assessment - The comparison of the inputs, processes, and outputs of a business function (and the dependencies of core business programs and processes on the function’s

outputs) to established assessment criteria to determine how critical the performance of the business function is to accomplishment of the agency's mission.

Critical Functions - Those business functions that must be restored in the event of a disruption to ensure the ability to protect the organization's assets, meet the organizational needs, and satisfy regulations.

Database - An aggregation of data; a file consisting of a number of records or tables, each of which is constructed of files of a particular type, together with a collection of operations that facilitate searching, sorting, recombination, and similar operations.

Data Communications - The movement of data between geographically separate locations via public and/or private electrical or optical transmission systems.

Defect - A problem or "bug" that if not removed, could cause a program to either produce erroneous results or otherwise fail.

Disaster - A sudden, unplanned calamitous event that causes great damage or loss. In the business environment, it is any event that creates an inability on an organization's part to provide the critical business functions for some predetermined period of time.

Disaster Mitigation - Activities taken to eliminate or reduce the degree of risk to life and property from hazards.

Disaster Preparedness - Activities, programs, and systems developed prior to a disaster that are used to support and enhance mitigation, response, and recovery to disasters.

Disaster Recovery - Activities and programs designed to return the entity to an acceptable condition.

Disaster Recovery Plan - An approved set of arrangements and procedures to enable an organization to respond to a disaster and resume its critical business functions within a defined time frame.

Disaster Recovery Planning - The process of developing advance arrangements and procedures which will enable an organization to respond to a disaster and resume the critical business functions within a predetermined period of time, minimize the amount of loss, and repair or replace the stricken facilities as soon as possible.

Disaster Response - Activities designed to address the immediate and short term effects of the disaster.

Electronic Vaulting - The transferring through telecommunications facilities of journaled transactions or data records to a remote backup location.

Event Horizon Date (Time Horizon To Failure) - The date when a risk may develop into a threat.

Hot Site - An alternate facility that has the equipment and resources to recover the critical business functions affected by the occurrence of a disaster. Hot sites may vary in the type of facilities offered such as data processing equipment, communications equipment, electrical power, etc.

Implementation Requirements - Pre-contingency, preparatory actions that must be accomplished so that the agency will have the ability to properly execute their BCP if conditions require it. Implementation requirements include such actions as: procuring any specialized equipment (e.g., cellular phones); obtaining any specialized software to support continuity operations (such as for a stand-alone PC activity); developing and stocking a supply of any forms required to support manual processing procedures; issuing support contracts, etc.).

Information Architecture - A description of the enterprise in terms of its business activity, business information, and their interaction.

Information Technology (IT) Applications - Applications (other than operating systems and other types of “firmware”) that are used to capture, process, and report data required in the performance of business functions. These include both critical and non-critical system applications.

Infrastructure - the computer and communication hardware, software, databases, people, facilities, and policies supporting the enterprise’s information management functions.

Integration Testing - Testing to determine that the related information system components perform to specification.

Interface - A boundary across which two systems communicate. An interface might be a hardware connector used to link to other devices, or it might be a convention used to allow communication between two software systems.

Inventory - In the context of a Year 2000 program, the process of determining the components that comprise the agency’s systems portfolio. The inventory should include all applications, databases, files, and related system components that will require inspection to locate data and related data computations.

Local Area Network (LAN) - A short distance network used to connect terminals, computers, and peripherals under some standard form, usually within one building or a group of buildings. A LAN does not make use of public carriers in linking together its components, although it may have a “gateway” outside the LAN that uses a public carrier.

Line Of Code - A single computer program command, declaration, or instruction. Program size is often measured in lines of code.

Loss - The unrecoverable business resources that are redirected or removed as a result of a disaster. Such losses may be loss of life, revenue, market share, competitive stature, public image, facilities, or operational capability.

Metrics - Measures by which processes, resources, and products can be assessed.

Mission-Critical System - A system supporting a core business activity or process.

Mitigate - To make or become milder, less severe, or less painful.

Offsite Storage - An alternate facility, other than the main facility, where duplicated vital records and documentation may be stored for use during recovery from a disaster.

Operating System - The software which schedules tasks, allocates storage, handles the interface to peripheral hardware, and presents a default interface to the user when no application program is running.

Outsourcing - Paying another company to provide services which an organization might otherwise have performed itself, e.g. software development.

Parallel Processing - The simultaneous use of more than one computer to solve a problem.

Planning Project Teams - Groups of people representing key organizational areas who are working together and following documented responsibilities for the design, development, and implementation of a business continuity plan.

Platform - The foundation technology of a computer system. Typically, a specific combination of hardware and operating system.

Portfolio - In the context of the Year 2000 program, a inventory, preferably automated, of an agency's information systems and their components grouped by business areas.

Production Environment - The system environment where the agency performs its routine information processing activities.

Project Management - The planning, organizing, and managing of tasks and resources to accomplish a defined objective, usually with constraints on time and cost.

Quality Assurance - All the planned and systematic actions necessary to provide adequate confidence that a product or service will satisfy given requirements for quality.

Reciprocal Agreement - An agreement between two organizations with basically the same equipment which allows one organization to process data for the other if it experiences a disaster.

Recovery Point Objective (RPO) - The point in time to which data must be restored in order to resume processing transactions.

Recovery Time Objective (RTO) - The maximum acceptable length of time that can elapse before the lack of a business function severely impacts the business entity. The RTO is comprised of two components; the time before a disaster is declared and the time to perform the tasks, as documented in the disaster recovery plan, to the point of business resumption.

Regression Testing - Selective retesting to detect faults introduced during modification of a system.

Relocatable Shell - A computer-ready cold site which can be transported to a disaster site so equipment can be obtained and installed near the original location.

Risk - The potential for failure or loss. Risk is measured in terms of probability/frequency and impact/severity for a specific risk condition.

Risk Assessment - An activity performed to identify risks and estimate their probability and the impact of their occurrence; it is used during system development to provide an estimate of damage, loss, or harm that could result from a failure to successfully develop individual system components. The process of identifying the risks to an organization, assessing the critical functions necessary for an organizations to continue business operations, defining the controls that are in place to reduce organization exposure, and evaluating the cost for such controls. The risk analysis often involves an evaluation of the probabilities of a particular event.

Risk Condition - A detailed description of the conditions that would result under planning assumptions. Conditions are defined as specific effects that the assumed situation would have on the inputs, threats from external events, and resources supporting the critical business function under study. A risk condition may be tied to Agency-wide risk scenarios.

Risk Management - A management approach designed to prevent and reduce risks, including system development risks, and lessen the impact of their occurrence.

Risk Scenarios - Macro-level Agency-wide conditions that may occur as a result of a Year 2000-related problem.

Standard - In computing, a set of detailed technical guidelines used as a means of establishing uniformity in an area of hardware or software development.

Strategic IRM Plan - A long-term, high-level plan that defines how the agency will use information technology to effectively accomplish the agency's missions, goals, and objectives.

Strategic Plan - A long-term, high-level plan that identifies broad business goals and provides a roadmap for their achievement.

Structured Walk-Through Exercise - A simulated method used to exercise or test a completed disaster recovery plan. Team members meet to verbally walk through each step of the plan to confirm the effectiveness of the plan and identify gaps, bottlenecks, or other plan weaknesses.

System Testing - Testing to determine that the results generated by the enterprise's information systems and their components are accurate and the systems perform to specification.

Telecommunications - Includes both voice and data communications. Literally, communicating at a distance. With respect to data communications it is a general term that applies to data that is transmitted by electrical, optical, or acoustical means between separate processing facilities.

Test - The process of exercising a product to identify differences between expected and actual behavior.

Test Facility - An environment that partially represents the production environment but is isolated from it, and is dedicated to the testing and validation of processes, applications, and system components.

Threat - The event that causes a risk to become a loss.

Trigger - Event(s) that cause a contingency plan to be activated (executed).

Unit Testing - Testing to determine that individual program modules perform to specification.

Validation - The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.

Warm Site - A partially equipped alternate site.

Wide Area Network (WAN) - A network which links metropolitan, campus, or local area networks across greater distances. Usually linked together by common carrier lines.

Year 2000 Compliant – With respect to information technology, Year 2000 compliant means that the information technology accurately processes data/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations, to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges data/time data with it.

Year 2000 Problem - The potential problems and its variations that might be encountered in any level of computer hardware and software from microcode to application programs, files, and databases that need to correctly interpret year-date data represented in 2-digit-year format. The problems are caused by computer programs which use only two digits to record the year (e.g., using "98" to represent 1998). Problems arise when attempts are made to process data for the year 2000 or after using only the last two digits. For example, most of the computer systems in use today will interpret a "00" entry as the year 1900. When this condition is experienced, the affected system will either compute erroneous information or simply stop working.

Appendix B

Business Continuity and Contingency Planning Template

Section 1: Business Process Inventory

1. Functional Area: ☐ HCFA Management (FA1)
☐ Program Development (FA2)
☐ Program Operations Management (FA3)
☐ Medicare Financial Management (FA4)
☐ Program Integrity (FA5)
☐ Medicaid and SCHIP Administration (FA6)
☐ External Communication (FA7)
☐ Administrative Services (FA8)
☐ Outreach and Education (FA9)
☐ Health Industry Standards (FA10)
☐ Program Quality (FA11)
2. Function:
3. Process:
4. Lead Component:
5. Lead Contact Person:
6. Lead Contact Phone #:
7. Other Involved Components:
8. Workgroup Jurisdiction:

<input type="checkbox"/> Program Integrity	<input type="checkbox"/> Payment Operations
<input type="checkbox"/> Quality of Care	<input type="checkbox"/> Enrollment
<input type="checkbox"/> Managed Care	<input type="checkbox"/> Litigation
<input type="checkbox"/> Telecommunications	<input type="checkbox"/> Infrastructure
<input type="checkbox"/> None	
9. Workgroup Contact Person:
10. Workgroup Contact Phone #:

Section 2: Business Process Analysis and Criticality

11. Description of Process:

12. Process Inputs:

13. Process Outputs:

14. Interdependencies with Other Processes/Systems:

15. Maximum Acceptable Outage:

16. Criticality Rating: ___ High ___ Medium ___ Low ___ Non-Critical

17. Rationale for Rating:

18. Decision Made by:

19. Component:

20. Phone #:

21. Date:

Section 3: Business Process Resource Dependencies

Resource Dependency #1

22. Name of Dependency:

23. Category: ☐ Information Application ☐ External Factor
 ☐ Human Resource ☐ Supporting Documentation
 ☐ Telecommunications ☐ ADP Infrastructure
 ☐ Physical Infrastructure

24. Level of Dependency: ☐ High ☐ Medium ☐ Low

Resource Dependency #2

25. Name of Dependency:

26. Category: ☐ Information Application ☐ External Factor
 ☐ Human Resource ☐ Supporting Documentation
 ☐ Telecommunications ☐ ADP Infrastructure
 ☐ Physical Infrastructure

27. Level of Dependency: ☐ High ☐ Medium ☐ Low

Resource Dependency #3

28. Name of Dependency:

29. Category: ☐ Information Application ☐ External Factor
 ☐ Human Resource ☐ Supporting Documentation
 ☐ Telecommunications ☐ ADP Infrastructure
 ☐ Physical Infrastructure

30. Level of Dependency: ☐ High ☐ Medium ☐ Low

Resource Dependency #4

31. Name of Dependency:

32. Category: ☐ Information Application ☐ External Factor
 ☐ Human Resource ☐ Supporting Documentation
 ☐ Telecommunications ☐ ADP Infrastructure
 ☐ Physical Infrastructure

33. Level of Dependency: ☐ High ☐ Medium ☐ Low

Resource Dependency #5

34. Name of Dependency:

35. Category: ☐ Information Application ☐ External Factor
 ☐ Human Resource ☐ Supporting Documentation
 ☐ Telecommunications ☐ ADP Infrastructure
 ☐ Physical Infrastructure

36. Level of Dependency: ☐ High ☐ Medium ☐ Low

37. Identified by:

38. Component:

39. Phone #:

Section 4: Risk Identification and Assessment

40. Risk Name:

41. Description of Risk:

42. Source of Risk (Name of Resource Dependency):

43. Affected Outputs and/or Functions:

44. Affected Users and/or Entities:

45. Probability of Occurrence: ☐ Certain ☐ Probable ☐ Possible
 ☐ Improbable

46. Rationale for Probability Estimate:

47. Impact of Occurrence: ☐ Catastrophic ☐ High ☐ Moderate
 ☐ Low

48. Rationale for Impact Estimate:

49. Proposed Response to Risk: ☐ Risk Mitigation Plan and Contingency Plan
 ☐ Contingency Plan
 ☐ Risk Mitigation Plan
 ☐ Watch

50. Rationale for Proposed Response:

51. Proposed by:

52. Component:

53. Phone #:

54. Date:

Section 5: Alternative Contingency Strategies

(Complete numbers 55 through 67 for each alternative.)

55. **CP Control Number:** To be Assigned by DACP
56. **CP Name:**
Distinguish alternate plans with suffixes, i.e. A, B, C
57. **CP Business Processes Addressed:**
List the Process numbers and names included in this CP
58. **CP Risks Addressed:**
List the risks (from Section 3 of the template) addressed by this CP. Specify critical systems (applications and hardware).
59. **CP Trigger Event:**
Specific failure that would precipitate this contingency plan
60. **CP Event Horizon Date:**
The date when a risk may develop into a threat
61. **CP Emergency Response Team (ERT):**
List the components, key individuals, titles and phone numbers who will be responsible for further developing this proposed plan, for assuring agency readiness on this proposed plan, for monitoring for Y2K failures and for executing this contingency plan. **Indicate Response Team Leader.**
62. **CP Decision Maker and Backup:**
Indicate who will be the decision maker for execution of this plan and who will be the backup if the former is not available. List the organizational component and the name and title of the individual who will be responsible for determining that the trigger point has been reached and that the contingency plan should be executed.
63. **CP Description of the Alternate Contingency Proposal:**
Describe the proposed plan, including primary actions to be undertaken by either HCFA CO or RO, contractors, states, PROS, etc. If the proposal includes phases of contingency plans (e.g. first phase is to attempt to fix the software), please address each major phase. Include the following:

Objective of the proposal:

Minimal Acceptable Level of Service provided by this proposal:

Strategy for Recovery Phase:

Strategy for Maintenance Phase:

Strategy for Restoration Phase:

64. **CP Cost Estimate:**

Provide the cost estimate for the proposal. (The estimated costs will be developed jointly by the workgroup/component and a team from OFM.) Provide brief explanation of how the costs are derived. Attach the cost estimate worksheet submitted to OFM and the completed spreadsheet and/or other documents prepared by OFM.

65. **CP Internal Clearances:** For each subject area, provide one of the following:

- a) Attach the workgroups/ component's request and a clearance/comment from the responsible component;
- b) State that no clearance was requested and why; or
- c) Clearance was requested but not received and why and attach the request for clearance.

Systems Security:	Assessment for systems security issues
Privacy Officer:	Assessment for privacy act issues
Program Integrity:	Assessment for program integrity concerns
Legal Counsel:	Assessment for litigative risk
Related/Dependent Component(s):	Clearance required by any 'downstream' components

66. **Submitted by:**
Workgroup/Component:
Name:
Phone #:
Date:

67. **CP Management Information: Checkoffs to allow sorting by: (yes/no)**

Carrier Involvement in CP execution:	Yes_____	No_____
Fiscal Intermediary Involvement in CP execution:	Yes_____	No_____
RO Involvement in CP monitoring/execution:	Yes_____	No_____
Contractor Front End Systems Involvement: :	Yes_____	No_____
Contractor Back End Systems Involvement: :	Yes_____	No_____
Standard System Involvement:	Yes_____	No_____
OIS/CO/Data Center Involvement:	Yes_____	No_____
CWF Involvement	Yes_____	No_____

Contractor Front End Systems Involvement means, editing, claims input, EDI etc. - Non standard system functions.

Contractor Back End Systems Involvement means check writing, payment distribution, EFT, accounting/financial etc. - Non standard system functions.

68. **Approved by EC:** Yes _____ No _____

69. **Date approved by EC:**

(After EC approval of a proposed Contingency Strategy, the above information, plus the additional information below will be used to draft the Agency's contingency plan.)

70. **Document each Phase and include the following:**

A. Plan to Recover the Business Process

1. **Description of Plan:**
2. **Objective:**
3. **Specific Actions (with Roles and Responsibilities):**
4. **Implementation Requirements:**
5. **Communication Mechanisms:**
6. **Anticipated Duration:**
7. **Exit Point (Conditions to Exit):**

B. Plan to Maintain Continuity of the Business

1. Description of Plan:
2. Objective:
3. Specific Actions (with Roles and Responsibilities):
4. Implementation Requirements:
5. Communication Mechanisms:
6. Anticipated Duration:
7. Exit Point (Conditions to Exit):

C. Plan to Restore Normal Business Operations

1. **Description of Plan:**
2. **Objective:**
3. **Specific Actions (with Roles and Responsibilities):**
4. **Implementation Requirements:**
5. **Communication Mechanisms:**
6. **Anticipated Duration:**
7. **Exit Point (Conditions to Exit):**

71. **CP Plan for Capturing Actual Execution Costs:**

Show how the agency will capture the actual execution costs from all parties involved in the plan, e.g. carriers, intermediaries, standard systems maintainers, PROs, HCFA CO and RO

72. **CP Plan for Monitoring Status:**

Indicate how the ERT will monitor for the trigger point for the contingency plan.

73. CP Project Plan:

Show a project plan for developing, testing, and monitoring through the readiness phase. Include beginning and ending dates for all major steps and the person(s) responsible. (The ERT will report regularly against this project plan.)

Section 6: Risk Mitigation Activity

74. **RM Control Number:** To be Assigned by DACP
75. **RM Name:**
76. **RM Business Processes Addressed:**
List the Process numbers and names included in this Risk Mitigation Plan
77. **RM Risks Addressed:**
List the risks (from Section 3 of the template) addressed by this Risk Mitigation Proposal
78. **RM Assessment of Current Level of Risk to this (these) processes:**
Comment on the nature of the risk(s) and the probability of problems if no action is taken to reduce the risk. Describe any actions taken to date to reduce risk.
79. **Risk Mitigation Team:**
List the components, and key individuals, who will be responsible for further developing and executing this risk mitigation plan. **Designate Team Leader.**
80. **RM Decision Maker:**
List the organizational component and the name and title of the individual who will be responsible for this risk mitigation plan.
81. **RM Description of Plan:**
Describe the proposed plan, including primary actions to be undertaken by either HCFA CO or RO, contractors, states, PROS, etc. Show the beginning and ending dates of all key activities. Describe the objectives of the proposed plan and how the actions in the proposal will reduce the risk of any failure in 2000.
82. **RM Cost Estimate:**
Provide the cost estimate for the plan. (The estimated costs will be developed jointly by the workgroup/component and a team from OFM.) Provide brief explanation of how the costs are derived. Attach the cost estimate worksheet submitted to OFM and the completed spreadsheet and/or other documents prepared by OFM.
83. **RM Internal Clearances:** For each subject area, provide one of the following:
- a) Attach the workgroups/ component's request and a clearance/comment from the responsible component;
 - b) State that no clearance was requested and why; or
 - c) Clearance was requested but not received and why and attach the request for clearance.

Systems Security: Assessment for systems security issues
Privacy Officer: Assessment for privacy act issues
Program Integrity: Assessment for program integrity concerns
Legal Counsel: Assessment for litigative risk
Related/Dependent Component(s): Clearance required by any 'downstream' components

84. **Submitted by:**
Workgroup/Component:
Name:
Phone #:
Date:

85. **RM Management Information: Checkoffs to allow sorting by: (yes/no)**

Carrier Involvement in RM execution:	Yes_____	No_____
Fiscal Intermediary Involvement in RM execution:	Yes_____	No_____
RO Involvement in RM monitoring/execution:	Yes_____	No_____
Contractor Front End Systems Involvement	Yes_____	No_____
Contractor Back End Systems Involvement:	Yes_____	No_____
Standard System Involvement:	Yes_____	No_____
OIS/CO/Data Center Involvement:	Yes_____	No_____
CWF Involvement	Yes_____	No_____

Contractor Front End Systems Involvement means, editing, claims input, EDI etc. - Non standard system functions.

Contractor Back End Systems Involvement means check writing, payment distribution, EFT, accounting/financial etc. - Non standard system functions.

86. **Approved by EC:**

87. **Date:**

(After EC approval of a proposed Risk Mitigation Plan, the above information, plus additional information below become part of the record for the Agency's Risk Mitigation Plan.)

88. **RM Plan for Capturing Actual Execution Costs:**

Show how the agency will capture the actual execution costs from all parties involved in the plan, e.g., carriers, intermediaries, standard systems maintainers, PROs, HCFA CO and Ros.

89. **RM Implementation Date:**

Beginning and End Dates

90. **RM Method for Ongoing Monitoring:**

INSTRUCTIONS FOR COMPLETING BUSINESS CONTINUITY AND CONTINGENCY PLANNING TEMPLATE

Background and General Instructions

HCFA and its business partners all have limited time and resources to continue normal operations while at the same time preparing our systems/processes for the millennium. Because of these limitations, we cannot develop contingency plans for every risk, but must limit our efforts to those risks that could lead to a stoppage or serious degradation of our core business functions. The most important of those functions are the ones assuring beneficiaries access to care, and, to that end, assuring providers are paid.

As a prerequisite to making a rational decision as to which risks require the development of a contingency plan, we must first inventory our critical business processes, identify the risks facing those processes, and assess the potential impact and probability of occurrence of each of those risks. To this end, we have structured our Business Continuity and Contingency Planning Template as follows:

Section 1: Business Process Inventory

Section 2: Business Process Analysis and Criticality

Section 3: Business Process Resource Dependencies

Section 4: Risk Identification and Assessment

Section 5: Risk Mitigation Activity

Section 6: Alternative Contingency Strategies

Section 7: Contingency Plan Development

Section 8: Contingency Plan Implementation

Section 1: Business Process Inventory

1. **Functional Area:** Select one of the following 11 HCFA functional areas listed in the Functional Inventory Working Draft (column 1).
 - HCFA Management (FA1)
 - Program Development (FA2)
 - Program Operations Management (FA3)
 - Medicare Financial Management (FA4)
 - Program Integrity (FA5)
 - Medicaid and SCHIP Administration (FA6)
 - External Communication (FA7)
 - Administrative Services (FA8)
 - Outreach and Education (FA9)
 - Health Industry Standards (FA10)
 - Program Quality (FA11)
2. **Function:** Select one of the functions (column 2) listed in the Functional Inventory Working Draft under the functional area you selected in item 1. Please provide function reference code (Fx.x) from Functional Inventory Working Draft.
3. **Process:** Select one of the processes (column 3) listed in the Functional Inventory Working Draft under the function you indicated in item 2. Please provide process reference code (Px.x.x) from Functional Inventory Working Draft.
4. **Lead Component:** Identify the HCFA organizational component with the lead responsibility for the process identified in item 3. Be as specific as possible (down to Group and Division level, if known).
5. **Lead Contact Person:** Identify the appropriate contact person in the lead component named in item 4.
6. **Lead Contact Phone #:** Provide the phone number for the individual named in item 5.
7. **Other Involved Components:** Identify any other organizational components with significant involvement in the process identified in item 3.
8. **Workgroup Jurisdiction:** Indicate which of the following cross-component contingency planning workgroups has jurisdiction for the process identified in item 3.

If you believe the process does not fall under any of the workgroups, select None and skip items 9 and 10.

- Program Integrity
- Payment Operations
- Quality of Care
- Enrollment
- Managed Care
- Litigation
- Telecommunications
- Infrastructure

9. **Workgroup Contact Person:** Identify the appropriate contact person on the workgroup indicated in item 8.
10. **Workgroup Contact Phone #:** Provide the phone number for the individual named in item 5.

Section 2: Business Process Analysis and Criticality

11. **Description of Process:** Provide a brief description of the business process identified in item 3.
12. **Process Inputs:** Provide a brief explanation of the major inputs to the process identified in item 3.
13. **Process Outputs:** Provide a brief explanation of the major outputs from the process identified in item 3.
14. **Interdependencies with Other Processes/Systems:** Provide a brief explanation of the interdependencies between the process identified in item 3 and other processes which may feed information into or depend upon information flowing out of the process under consideration.
15. **Maximum Acceptable Outage:** Describe the greatest level of functional degradation that could occur in the process identified in item 3 and still yield minimally acceptable results.
16. **Criticality Rating:** Select the appropriate rating in accordance with the following criteria.
 - **High** - The extended failure of the process would (1) prohibit the performance of the Agency's core business functions and programs, (2) impede mission accomplishment, (3) adversely impact and jeopardize business partners' mission accomplishment; and/or (4) negatively impact the national and global economies.
 - **Medium** - The extended failure of the process would adversely affect Agency operations to the extent that (1) the ability to support core business functions and programs would be seriously impaired, (2) mission accomplishment would be jeopardized, (3) relations with business partners would be strained; and/or (4) there would be a potential negative impact on national and global economies.
 - **Low** - The extended failure of the process would adversely impact day-to-day operations of the Agency, and could, over time, degrade support to core business functions and programs.
 - **Non-Critical** - The extended failure of the process would impact day-to-day operations; however, it would not impair support of core business functions and programs, and affected operations could cope with reduced

capabilities.

17. **Rationale for Rating:** Provide an explanation for the criticality rating selected in item 16.
18. **Decision Made by:** Provide the name of the individual who determined the criticality rating.
19. **Component:** Specify the organizational component of the individual named in item 18.
20. **Phone #:** Provide the phone number of the individual named in item 18.
21. **Date:** Provide the date on which the criticality rating decision was made.

Section 3: Business Process Resource Dependencies

Report in this section information on the resources and external factors upon which the business process identified in item 3 is dependent.

- 22. Name of Dependency:** Briefly describe the nature of the resource/external factor dependency.
- 23. Category:** Select the category into which the dependency named in item 13 best fits from among the following.
- Information Application
 - External Factors (input and external events)
 - Human Resources
 - Supporting Documentation
 - Telecommunications
 - ADP Infrastructure
 - Physical Infrastructure
- 24. Level of Dependency:** Indicate whether the level of dependency is High, Medium, or Low in accordance with the following criteria.
- **High** - Resources that are used frequently in day-to-day operations and are essential to the proper accomplishment of critical business requirements.
 - **Medium** - Resources that are used during the normal course of critical business operations, but whose immediate availability is not essential.
 - **Low** - Resources that are only occasionally used in day-to-day operations and are not essential to actually accomplishing critical business requirements.
- 25-36:** Space is provided for you to report up to 4 more resource dependencies utilizing the same instructions as for items 22-24.
- 37. Identified by:** Provide the name of the individual who identified the resource dependencies.
- 38. Component:** Specify the organizational component of the individual named in item 37.
- 39. Phone #:** Provide the phone number of the individual named in item 37.

Section 4: Risk Identification and Assessment

40. **Risk Name:** Provide a brief name for the risk identified.
41. **Description of Risk:** Explain the negative thing may happen, to which you have to respond. This should not be a routine problem of project and schedule management. The identified risk should be stated in terms of some event, constraint, or other factor that would force you to not perform a business process at a needed level.
42. **Source of Risk (Name of Resource Dependency):** Describe the source of the risk, relating it the one of the resource dependencies of the process at risk identified in Section 3.
43. **Affected Outputs and/or Functions:** Specify those process and system outputs and/or business functions that will be effected by occurrence of the risk and explain how they will be affected.
44. **Affected Users and/or Entities:** Indicate the HCFA users and/or external entities (e.g., beneficiaries, providers, banks, data exchange partners) most likely and most seriously to be affected by the occurrence of the risk.
45. **Probability of Occurrence:** Indicate the probability that the risk will occur by selecting one of the following levels of likelihood where p equals the probability of occurrence:
- ◆ Certain = $90\% < p < 100\%$;
 - ◆ Probable = $50\% < p < 90\%$;
 - ◆ Possible = $10\% < p < 50\%$; or
 - ◆ Improbable = $0\% < p < 10\%$.

We recognize that you will not be able to calculate the precise percentage of probability and are providing these categories only to ensure that all planners will at least be using the same range of values in making their estimates.

46. **Rationale for Probability Estimate:** Explain the basis for your choice of probability categories.
47. **Impact of Occurrence:** Select the level of impact that the occurrence of the risk would entail for core Medicare business operations from the following choices: Catastrophic, High, Moderate, Low. We would define **Catastrophic** to be those risks that could lead to a total failure or serious degradation in a Medicare core

business function. Risks with **High** impact would be those that could impair the performance of Medicare business functions, even to the point of potential political embarrassment, but not to a degree likely to affect life or financial survival. **Moderate** risks would have some noticeable impact on some sector of operations, and **Low** impact risks very little effect of any import.

48. Rationale for Impact Assessment: Explain your basis for the choice of impact category you selected. Quantify the expected impact to the degree possible (e.g., the potential costs and expected duration of any service disruptions).

49. Proposed Response to Risk: Select your proposed response for dealing with the risk from the following categories.

- ◆ **Risk Mitigation Plan and Contingency Plan** - pursue risk mitigation activities while simultaneously developing a detailed contingency plan.
- ◆ **Contingency Plan** - develop a detailed contingency plan.
- ◆ **Risk Mitigation Plan** - pursue risk mitigation activities.
- ◆ **Watch** - no active plan other than keeping an eye on the risk in case events cause its likelihood or potential impact to increase significantly.

IMPACT PROBABILITY	CATASTROPHIC	HIGH	MODERATE	LOW
CERTAIN	RM and CP	RM and CP	CP	RM or CP
PROBABLE	RM and CP	RM and CP	RM or CP	Watch
POSSIBLE	CP	CP	RM or CP	Watch
IMPROBABLE	CP	RM or CP	Watch	Watch

RM = Risk Mitigation **CP** = Contingency Plan **W** = Watch

50. Rationale for Proposed Response: Justify your proposed course of action, keeping in mind where the risk falls on the following risk assessment matrix which balances relative risk impact against probability of risk occurrence.

The above matrix provides a guideline for determining the proper response to a given risk based upon its expected impact and the probability of its occurrence.

RM and CP: These risks are the most serious and/or most likely to occur. They require the development of an active risk mitigation plan to avoid the negative impact that may occur, as well as a contingency plan to counteract the risk if it does occur.

CP: The anticipated impact of these risks is severe enough to mandate the development of a contingency plan for dealing with them, even though the probability of their occurrence may be something less than certain.

RM or CP: These risks have sufficiently serious impact and are likely enough to occur to warrant a planned response of some sort: either an active risk mitigation plan or a detailed contingency plan. The more appropriate of the two responses must be determined based upon the nature of the individual risk.

Watch: These risks are of sufficiently low impact and/or unlikely enough to occur that no active plan is required other than keeping an eye on the potential risk in case events cause its risk/probability status to rise significantly.

Section 5: Alternative Contingency Strategies

Report in this section information on alternative approaches for working around problems caused by occurrence of the risk identified in Section 4, Item 40, for continuing the performance of critical business functions despite the loss of resources, and the effects caused by external factors.

(Complete numbers 55 through 67 for each alternative.)

55. **CP Control Number:** To be Assigned by DACP

56. **CP Name:**

Provide a brief name for the alternate contingency strategy. Distinguish alternate plans with suffixes, i.e. A, B, C

57. **CP Business Processes Addressed:**

List all Process numbers and names addressed in alternate contingency strategy.

58. **CP Risks Addressed:**

List the risks (from Section 3 of the template) addressed in alternate contingency strategy. Specify critical systems (applications and hardware).

59. **CP Trigger Event:**

Specific failure that would precipitate this contingency plan.

60. **CP Event Horizon Date:**

The date when a risk may develop into a threat.

61. **CP Emergency Response Team (ERT):**

List the components, key individuals, titles and phone numbers of those who will be responsible for further developing this proposed plan, for assuring agency readiness on this proposed plan, for monitoring for Y2K failures and for executing this contingency plan. **Indicate Response Team Leader.**

62. **CP Decision Maker and Backup:**

Indicate who will be the decision maker for execution of this plan and who will be the backup (if the former is not available). List the organizational component and

the name and title of the individual who will be responsible for determining that the trigger point has been reached and that the contingency plan should be executed.

63. CP Description of the Alternate Contingency Proposal:

Describe the proposed plan, including primary actions to be undertaken by either HCFA CO or RO, contractors, States, PROS, etc. If the proposal includes phases of contingency plans (e.g. first phase is to attempt to fix the software), please address each major phase. Include the following:

Objective of the proposal:

Minimal Acceptable Level of Service provided by this proposal:

Strategy for Recovery Phase:

Strategy for Maintenance Phase:

Strategy for Restoration Phase:

64. CP Cost Estimate:

Provide the cost estimate for the proposal. (The estimated costs will be developed jointly by the workgroup/component and a team from OFM.) Provide brief explanation of how the costs are derived. Attach the cost estimate worksheet submitted to OFM and the completed spreadsheet and/or other documents prepared by OFM.

65. CP Internal Clearances: For each subject area, provide one of the following:

- a) Attach the workgroups/component's request and a clearance/comment from the responsible component;
- b) State that no clearance was requested and why; or
- c) Clearance was requested but not received and why (attach the request for clearance).

Systems Security:	Assessment for systems security issues
Privacy Officer:	Assessment for privacy act issues
Program Integrity:	Assessment for program integrity concerns
Legal Counsel:	Assessment for litigative risk
Related/Dependent Component(s):	Clearance required by any 'downstream' components

66. **Submitted by:**
Workgroup/Component:
Name:
Phone #:
Date:

67. **CP Management Information: Checkoffs to allow sorting by: (yes/no)**

Carrier Involvement in CP execution:	Yes_____	No_____
Fiscal Intermediary Involvement in CP execution:	Yes_____	No_____
RO Involvement in CP monitoring/execution:	Yes_____	No_____
Contractor Front End Systems Involvement:	Yes_____	No_____
Contractor Back End Systems Involvement:	Yes_____	No_____
Standard System Involvement:	Yes_____	No_____
OIS/CO/Data Center Involvement:	Yes_____	No_____
CWF Involvement	Yes_____	No_____

Contractor Front End Systems Involvement means, editing, claims input, EDI, etc. - Non standard system functions.

Contractor Back End Systems Involvement means check writing, payment distribution, EFT, accounting/financial, etc. - Non standard system functions.

68. **Approved by EC:** Yes _____ No _____
69. **Date approved by EC:**

(After EC approval of a proposed Contingency Strategy, the above information, plus the additional information below will become the Agency's contingency plan.)

70. **Document each Phase and include the following:**

A. Plan to Recover the Business Process

1. Description of Plan:
2. Objective:
3. Specific Actions (with Roles and Responsibilities):
4. Implementation Requirements:
5. Communication Mechanisms:
6. Anticipated Duration:
7. Exit Point (Conditions to Exit):

B. Plan to Maintain Continuity of the Business

1. Description of Plan:
2. Objective:
3. Specific Actions (with Roles and Responsibilities):
4. Implementation Requirements:

5. Communication Mechanisms:
6. Anticipated Duration:
7. Exit Point (Conditions to Exit):

C. Plan to Restore Normal Business Operations

1. Description of Plan:
2. Objective:
3. Specific Actions (with Roles and Responsibilities):
4. Implementation Requirements:
5. Communication Mechanisms:
6. Anticipated Duration:
7. Exit Point (Conditions to Exit)

71. CP Plan for Capturing Actual Execution Costs:

Show how the agency will capture the actual execution costs from all parties involved in the plan, e.g. carriers, intermediaries, standard systems maintainers, PROs, HCFA CO and RO

72. CP Plan for Monitoring Status:

Indicate how the ERT will monitor for the trigger point for the contingency plan.

73. CP Project Plan:

Show a project plan for developing, testing, and monitoring through the readiness phase. Include beginning and ending dates for all major steps and the person(s) responsible. (The ERT will report regularly against this project plan.)

Section 6: Risk Mitigation Activity

Report in this section information on risk mitigation plans and activities that will be invoked. Provide a summary of what you expect to do to avoid the occurrence/failure threatened by the risk identified in Section 4, Item 40, in order to prevent a contingency plan from being needed. For example, you may have identified a significant risk of schedule failure for completing testing; your mitigation plan would identify the measures you will take to keep that from becoming an actual implementation or production failure.

74. **RM Control Number:** To be Assigned by DACP

75. **RM Name:**

Provide a brief name for the Risk Mitigation Plan.

76. **RM Business Processes Addressed:**

List all Process numbers and names addressed in this Risk Mitigation Plan.

77. **RM Risks Addressed:**

List the risks (from Section 3 of the template) addressed by this Risk Mitigation Plan.

78. **RM Assessment of Current Level of Risk to this (these) processes:**

Comment on the nature of the risk(s) and the probability of problems if no action is taken to reduce the risk. Describe any actions taken to date to reduce risk.

79. **Risk Mitigation Team:**

List the components, and key individuals, who will be responsible for further developing and executing this risk mitigation plan. **Designate Team Leader.**

80. **RM Decision Maker:**

List the organizational component and the name and title of the individual who will be responsible for this risk mitigation plan.

81. **RM Description of Plan:**

Describe the proposed plan, including primary actions to be undertaken by either HCFA CO or RO, contractors, states, PROS, etc. Show the beginning and

ending dates of all key activities. Describe the objectives of the proposed plan and how the actions in the proposal will reduce the risk of any failure in 2000.

82. RM Cost Estimate:

Provide the cost estimate for the plan. (The estimated costs will be developed jointly by the workgroup/component and a team from OFM.) Provide brief explanation of how the costs are derived. Attach the cost estimate worksheet submitted to OFM and the completed spreadsheet and/or other documents prepared by OFM.

83. RM Internal Clearances: For each subject area, provide one of the following:

- a) Attach the workgroups/ component's request and a clearance/comment from the responsible component;
- b) State that no clearance was requested and why; or
- c) Clearance was requested but not received and why and attach the request for clearance.

Systems Security:	Assessment for systems security issues
Privacy Officer:	Assessment for privacy act issues
Program Integrity:	Assessment for program integrity concerns
Legal Counsel:	Assessment for litigative risk
Related/Dependent Component(s):	Clearance required by any 'downstream' components

84. Submitted by:
Workgroup/Component:
Name:
Phone #:
Date:

85. RM Management Information: Checkoffs to allow sorting by: (yes/no)

Carrier Involvement in CP execution:	Yes_____	No_____
Fiscal Intermediary Involvement in CP execution:	Yes_____	No_____
RO Involvement in CP monitoring/execution:	Yes_____	No_____
Contractor Front End Systems Involvement:	Yes_____	No_____
Contractor Back End Systems Involvement:	Yes_____	No_____
Standard System Involvement:	Yes_____	No_____
OIS/CO/Data Center Involvement:	Yes_____	No_____
CWF Involvement	Yes_____	No_____

Contractor Front End Systems Involvement means, editing, claims input, EDI etc. - Non standard system functions.

Contractor Back End Systems Involvement means check writing, payment distribution, EFT, accounting/financial etc. - Non standard system functions.

86. **Approved by EC:**

87. **Date:**

(After EC approval of a proposed Risk Mitigation Plan, the above information, plus additional information below become part of the record for the Agency's Risk Mitigation Plan.)

88. **RM Plan for Capturing Actual Execution Costs:**

Show how the agency will capture the actual execution costs from all parties involved in the plan, e.g., carriers, intermediaries, standard systems maintainers, PROs, HCFA CO and Ros.

89. **RM Implementation Date:**

Beginning and End Dates

90. **RM Method for Ongoing Monitoring:**

Show a project plan for monitoring of the Risk Mitigation Plan. Include information/documentation to indicate if the Risk Mitigation Plan is performing as expected and steps that may need to be taken if plan does not have the expected results.

Appendix D

Final Contingency Plan Outline

Control Number: To be Assigned by DACP

Name:

3.3 Scope:

1.0 **Business Processes Addressed:** List the Process numbers and names included in this CP.

1.1 **Risks Addressed:** List the risks (from Section 3 of the template) addressed by this CP. Specify critical systems (applications and hardware).

2.0 Trigger:

3.3 **Event:** Specific failure that would precipitate this contingency plan.

3.3 **Plan for Monitoring Status:** Indicate how the ERT will monitor for the trigger point for the contingency plan.

3.3 **Event Horizon Date:** The date when a risk may develop into a threat.

3.0 Contingency Planners:

3.1 **Emergency Response Team (ERT):** List the components, key individuals, titles and phone numbers who will be responsible for further developing this proposed plan, for assuring agency readiness on this proposed plan, for monitoring for Y2K failures and for executing this contingency plan. **Indicate Response Team Leader.**

3.2 **Decision Maker and Backup:** Indicate who will be the decision maker for execution of this plan and who will be the backup if the former is not available. List the organizational component and the name and title of the individual who will be responsible for determining that the trigger point has been reached and that the contingency plan should be executed.

4.0 Contingency Plan:

4.1 Plan to Recover the Business Process

4.1.1 **Description of Plan:**

4.1.2 **Objective:**

4.1.3 **Specific Actions (with Roles and Responsibilities):**

4.1.4 **Implementation Requirements:**

4.1.5 **Communication Mechanisms:**

4.1.6 **Anticipated Duration:**

4.1.7 **Exit Point (Conditions to Exit):**

4.2 Plan to Maintain Continuity of the Business

4.2.1 **Description of Plan:**

4.2.2 **Objective:**

4.2.3 **Specific Actions (with Roles and Responsibilities):**

4.2.4 **Implementation Requirements:**

4.2.5 **Communication Mechanisms:**

4.2.6 **Anticipated Duration:**

4.2.7 **Exit Point (Conditions to Exit):**

4.3 Plan to Restore Normal Business Operations

4.3.1 **Description of Plan:**

4.3.2 **Objective:**

4.3.3 **Specific Actions (with Roles and Responsibilities):**

4.3.4 **Implementation Requirements:**

4.3.5 **Communication Mechanisms:**

4.3.6 **Anticipated Duration:**

4.3.7 **Exit Point (Conditions to Exit):**

5.0 Internal and External Interrelationships (check if applicable):

Carrier Involvement in CP execution:	<input type="checkbox"/>
Fiscal Intermediary Involvement in CP execution:	<input type="checkbox"/>
RO Involvement in CP monitoring/execution:	<input type="checkbox"/>
Contractor Front End Systems Involvement (editing, claims input, EDI etc. - Non standard system functions):	<input type="checkbox"/>
Contractor Back End Systems Involvement (check writing, payment distribution, EFT, accounting/financial etc. - Non standard system functions):	<input type="checkbox"/>
Standard System Involvement:	<input type="checkbox"/>
OIS/CO/Data Center Involvement:	<input type="checkbox"/>
CWF Involvement:	<input type="checkbox"/>

6.0 Plan for Capturing Actual Execution Costs: Show how the Agency will capture the actual execution costs from all parties involved in the plan (e.g., carriers, intermediaries, standard system maintainers, PROs, HCFA CO and RO, etc.)

7.0 Responsible Entity:

7.1 Submitted by:
7.2 Workgroup/Component:
7.3 Name:
7.4 Phone #:
7.5 Date:

Append additional information (i.e., recall rosters; vendor addresses, phone numbers, fax numbers, and contract information; alternate facility maps, etc.) as necessary.

Appendix E

Final Risk Mitigation Plan Outline

Control Number: To be Assigned by DACP

Name:

1.0 Scope:

1.1 Business Processes Addressed: List the Process numbers and names included in this Risk Mitigation Plan.

1.2 Risks Addressed: List the risks (from Section 3 of the template) addressed by this Risk Mitigation Plan.

2.0 Risk Mitigation Assessment of Current Level of Risk to Processes Addressed: Comment on the nature of the risk(s) and the probability of problems if no action is taken to reduce the risk. Describe any actions already taken to reduce the risk.

3.0 Risk Mitigation Planners:

3.1 Risk Mitigation Team: List the components, key individuals, titles and phone numbers who will be responsible for further developing or implementing this plan. **Designate a Team Leader.**

3.2 Risk Mitigation Decision Maker: List the organizational component and the name and title of the individual who will be responsible for this risk mitigation plan.

4.0 Risk Mitigation Plan: Describe the risk mitigation plan, including primary actions to be undertaken by either HCFA CO or RO, contractors, states, PROs, etc. Show the beginning and ending dates of all key activities. Describe the objectives of the plan and how the actions will reduce the risk of any Y2k failure.

5.0 Implementation and Ongoing Monitoring:

5.1 Implementation Dates: Beginning and End Dates

5.2 Method for Ongoing Monitoring:

6.0 Internal and External Interrelationships (check if applicable):

Carrier Involvement in RM execution: ☐

Fiscal Intermediary Involvement in RM execution: ☐

RO Involvement in RM monitoring/execution: ☐

Contractor Front End Systems Involvement ☐

(editing, claims input, EDI etc. - Non standard system functions):

Contractor Back End Systems Involvement (check ☐

writing, payment distribution, EFT, accounting/financial etc. - Non standard system functions):

Standard System Involvement: ☐

OIS/CO/Data Center Involvement: ☐

CWF Involvement: ☐

7.0 Plan for Capturing Actual Execution Costs: Show how the Agency will capture the actual execution costs from all parties involved in the plan (e.g., carriers, intermediaries, standard system maintainers, PROs, HCFA CO and RO, etc.)

8.0 Responsible Entity:

- 8.1 Submitted by:
- 8.2 Workgroup/Component:
- 8.3 Name:
- 8.4 Phone #:
- 8.5 Date:

Append additional information as necessary.